VMware View 管理员指南

View 4.5

View Manager 4.5

View Composer 2.5

在本文档被更新的版本替代之前，本文档支持列出的每个产品的版本和所有后续版本。要查看本文档的更新版本，请访问 http://www.vmware.com/cn/support/pubs。

ZH_CN-000244-00

vmware®

最新的技术文档可以从 VMware 网站下载：

http://www.vmware.com/cn/support/pubs/

VMware 网站还提供最近的产品更新信息。

您如果对本文档有任何意见或建议，请把反馈信息提交至：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

北京办公室
北京市海淀区科学院南路 2 号
融科资讯中心 C 座南 8 层
www.vmware.com/cn

上海办公室
上海市浦东新区浦东南路 999 号
新梅联合广场 23 楼
www.vmware.com/cn

广州办公室
广州市天河北路 233 号
中信广场 7401 室
www.vmware.com/cn

目录

关于本书

*《VMware View 管理员指南》*介绍了如何配置和管理 VMware View™，其中包括如何配置 View Connection Server、如何创建管理员、如何部署 View 桌面、如何设置用户身份验证、如何配置策略以及如何在 View Administrator 中管理 VMware ThinApp™。本指南还介绍了如何对 VMware View 组件进行维护和故障排除。

目标读者

本指南面向任何需要配置和管理 VMware View 的人员。本指南中的信息针对熟练掌握虚拟机技术和数据中心操作、并具有丰富经验的 Windows 或 Linux 系统管理员。

VMware 技术刊物词汇表

VMware® 技术刊物中提供了您可能不太熟悉的术语词汇表。有关 VMware 技术文档中所用术语的定义，请访问 http://www.vmware.com/cn/support/pubs。

文档反馈意见

VMware 欢迎您提供文档改进意见和建议。如有任何意见或建议，请将反馈信息提交至以下地址：docfeedback@vmware.com。

技术支持与培训资源

下面列出了您可利用的技术支持资源。要获取本书以及其他书籍的最新版本，请访问 http://www.vmware.com/cn/support/pubs。

在线支持和电话支持

要通过在线支持提交您的技术支持请求，请查看产品及合同信息，并对产品进行注册，然后访问 http://www.vmware.com/cn/support。

对于优先级最高的问题，已签署相应支持合同的客户应使用电话支持，以最快地获得支持。请访问 http://www.vmware.com/cn/support/phone_support.html。

支持服务

要了解 VMware 支持服务如何帮助满足您的业务需求，请访问 http://www.vmware.com/cn/support/services。

VMware 专业服务

VMware 培训服务课程提供了丰富的实践练习、案例研究示例和课程材料，可用作您工作中的参考工具。培训形式多样，包括现场授课、课堂培训以及实时网络教学。对于现场指导项目和最佳操作方法，VMware 咨询服务提供了多种服务，帮助您评估、规划、构建和管理您的虚拟环境。要获取有关培训课程、认证计划以及咨询服务的信息，请访问 http://www.vmware.com/cn/services。

配置 View Connection Server 1

当您安装 View Connection Server 并对其执行初始配置后，可以向 View Manager 中添加 vCenter Server 实例和 View Composer 服务，设置可委托管理员职责的角色，以及安排配置数据的备份。

本章讨论了以下主题：

使用 View Administrator

View Administrator 是一个 Web 界面，您可以通过此界面配置 View Connection Server 并管理 View 桌面。

有关您使用 View Administrator、View cmdlets 和 `vdmadmin` 所能执行操作的对比，请参阅《*VMware View Integration Guide*》（VMware View 集成指南）。

View Administrator 和 View Connection Server

View Administrator 为 View Manager 提供管理界面。

根据您的 View 部署，可能需要一个或多个 View Administrator 界面。

- 使用一个 View Administrator 界面，管理与一个独立的 View Connection Server 实例或一个副本 View Connection Server 实例组相关联的 View 组件。

  您可以使用任何一个副本实例的 IP 地址登录 View Administrator。

- 您必须使用一个单独的 View Administrator 界面来管理各个独立的 View Connection Server 实例以及各组副本 View Connection Server 实例的 View 组件。

此外，还要使用 View Administrator 来管理与 View Connection Server 相关联的安全服务器和 View Transfer Server 实例。

- 每个安全服务器与一个 View Connection Server 实例相关联。
- 每个 View Transfer Server 实例可以与副本实例组中的任意 View Connection Server 实例进行通信。

登录 View Administrator

要执行初始配置任务，您必须登录 View Administrator。

前提条件

- 确认 View Connection Server 安装在专用计算机上。
- 确认您使用的是 View Administrator 支持的 Web 浏览器。有关 View Administrator 需求，请参阅*《VMware View 安装指南》*。

步骤

1 打开 Web 浏览器并输入以下 URL，其中 *服务器* 是 View Connection Server 实例的主机名或 IP 地址。

https://*服务器*/admin

您可以通过安全连接 (SSL) 来访问 View Administrator。当您第一次连接时，Web 浏览器可能会显示一个页面，警告与该地址相关联的安全证书不是由受信任的证书颁发机构颁发的。这是正常现象，因为 View Connection Server 附带的默认证书是一个自签证书。

2 单击 **[Ignore（忽略）]** 继续使用当前 SSL 证书。

3 使用 View Connection Server 计算机上的管理员凭据登录。

最初，View Connection Server 计算机中本地管理员组 (BUILTIN\Administrators) 的所有成员用户都可以登录 View Administrator。

登录 View Administrator 后，您可以使用 **[View Configuration（View 配置）] > [Administrators（管理员）]** 来更改 View Manager 管理员列表。

有关使用 View Administrator 界面的提示

您可以使用 View Administrator 用户界面的功能浏览 View 页面以及查找、过滤和排序 View 对象。

View Administrator 中包含许多常见用户界面功能。例如，每个页面左侧的导航窗格都可将您引导至其他 View Administrator 页面。使用搜索过滤器可以选择与搜索对象相关的过滤条件。

表 1-1 描述了其他一些可帮助您使用 View Administrator 功能。

表 1–1 View Administrator 导航和显示功能

View Administrator 功能	描述
在 View Administrator 页面中前后导航。	单击 View Administrator 页面左上角的 **[Back（返回）]** 按钮可返回显示的上一页 View Administrator 页面。单击 **[Forward（前进）]** 按钮返回当前页面。 不要使用浏览器的 **[Back（返回）]** 按钮。此按钮将显示 View Administrator 的登录页面。
多列排序	通过使用多列排序功能，您可以按多种方式对 View 对象进行排序。 单击 View Administrator 表第一行中的标题，可根据该标题按字母顺序对 View 对象进行排序。 例如，在 **[Inventory（清单）] > [Desktops（桌面）]** 页面上，您可以单击 **[Pool（池）]**，按照包含桌面的池对桌面进行排序。 数字 **1** 将显示在标题旁边，表示它是主要排序列。您可以再次单击该标题，以便反转排序顺序。排序顺序由向上或向下箭头表示。 要使用辅助项对 View 对象进行排序，请按住 Ctrl 键并单击另一个标题。 例如，在 **[Desktops（桌面）]** 表中，您可以单击 **[Users（用户）]**，根据桌面专属的用户执行辅助排序。数字 **2** 将显示在辅助标题旁边。在此示例中，桌面将按池以及每个池中的用户进行排序。 您可以继续按住 Ctrl 键按重要性对表中的所有列进行降序排序。 按下 Ctrl+Shift 组合键同时单击某个排序项可将该项取消。 例如，您可能希望显示池中处于特定状态且存储在特定数据存储中的桌面。您可以依次单击 **[Inventory（清单）] > [Pools（池）]**、池 ID、**[Datastore（数据存储）]** 标题，然后按住 Ctrl 键并单击 **[Status（状态）]** 标题。
选择 View 对象并显示 View 对象的详细信息	在列出 View 对象的 View Administrator 表中，可以选择对象或显示其详细信息。 ■ 要选择一个对象，请在表中单击该对象行的任意位置。在页面顶端，用来管理该对象的菜单和命令将会激活。 ■ 要显示对象详细信息，请双击对象行中的左侧单元格。此时将出现一个新的页面，其中会显示该对象的详细信息。 例如，在 **[Inventory（清单）] > [Pools（池）]** 页面上，单击某个池的行中的任意位置，即可激活影响该池的命令。 双击左侧列中的 **[Pool ID（池 ID）]** 单元格将显示一个新的页面，其中包含了该池的详细信息。
展开对话框以查看详细信息	您可以展开 View Administrator 对话框以查看详细信息，如表列中的桌面名称和用户名。 要展开对话框，请将鼠标放在对话框右下角的点上并拖动该角。

排除不通过安全 SSL 连接访问 View Administrator 时出现的故障

当 View 客户端的 SSL 设置与您用来连接 View Administrator 的 URL 不一致时，您无法通过 Web 浏览器登录 View Administrator。如果您取消选择 SSL 设置，您将无法在 URL 中使用 `https`。

问题

您用来登录 View Administrator 的 URL 不再可用。连接失败。

原因

默认情况下，View Manager 使用 SSL 在 View 客户端与 View Connection Server 之间创建安全连接。此设置还适用于通过 Web 浏览器连接 View Administrator 的计算机。

当您导航到 **[View Configuration（View 配置）] > [Global Settings（全局设置）]** 并取消选中 **[Require SSL for client connections and View Administrator（需要将 SSL 用于客户端连接和 View Administrator）]** 复选框，从而在 View Administrator 中更改此设置时，会出现此问题。

解决方案

请使用以下 URL 连接 View Administrator，其中<*服务器*>是 View Connection Server 实例的主机名或 IP 地址。

http://<*服务器*>/admin

排除 View Administrator 中的文本显示故障

如果您的 Web 浏览器在非 Windows 操作系统（如 Linux、UNIX 或 Mac OS）上运行，View Administrator 中的文本会无法正常显示。

问题

View Administrator 界面中的文本显示为乱码。例如，单词中间出现空格。

原因

View Administrator 需要使用 Microsoft 专用字体。

解决方案

在计算机上安装 Microsoft 专用字体。

目前，Microsoft 网站不提供 Microsoft 字体，但您可以从其他独立网站进行下载。

配置 vCenter Server 和 View Composer

要将虚拟机用作桌面源，必须配置 View Manager，使其与 vCenter Server 通信。要创建和管理链接克隆桌面，必须在 View Manager 中配置 View Composer 设置。

将 vCenter Server 实例添加到 View Manager

必须配置 View Manager，使其连接到 View 部署中的 vCenter Server 实例。vCenter Server 可创建和管理 View Manager 用作桌面源的虚拟机。

前提条件

- 安装 View Connection Server 产品许可证密钥。
- 准备一个具有权限的 vCenter Server 用户，以便在 vCenter Server 中执行支持 View Manager 所需的操作。要使用 View Composer，您必须授予该用户额外的特权。要管理以本地模式使用的桌面，除 View Manager 和 View Composer 中所需的特权外，您还必须为用户授予额外特权。

  有关为 View Manager 配置 vCenter Server 用户的详细信息，请参阅《*VMware View 安装指南*》。

步骤

1. 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。
2. 在 [vCenter Server] 面板中，单击 **[Add（添加）]**。
3. 在服务器地址文本框中，键入 vCenter Server 实例的主机域名全称 (FQDN) 或 IP 地址。

   FQDN 包括主机名称和域名。例如，在 FQDN **myserverhost.companydomain.com** 中，**myserverhost** 是主机名称，而 **companydomain.com** 是域名。

   注意 如果您通过 DNS 名称或 URL 来输入服务器，则 View Manager 不会执行 DNS 查找来确认管理员之前是否使用 IP 地址将服务器添加到 View Manager 中的。如果同时使用 DNS 名称和 IP 地址添加 vCenter Server，则会发生冲突。

4. 键入 vCenter Server 用户的名称。
5. 键入 vCenter Server 用户密码。

6 （可选）键入此 vCenter Server 实例的描述。

7 要使用安全通道 (SSL) 连接到 vCenter Server，确保选中 **[Connect using SSL（使用 SSL 连接）]**。SSL 连接是默认设置。

8 键入 TCP 端口号。

   默认端口为 443。

9 （可选）单击 **[Advanced（高级）]** 配置 vCenter Server 中的最大并发池操作数量。

   a 设置并发部署操作的最大数量。

      此设置确定 View Manager 可在此 vCenterServer 实例中创建完整虚拟机的并发请求最大数。默认值为 8。此设置不控制链接克隆部署。

   b 设置并发电源操作的最大数量。

      此设置确定此 vCenter Server 实例中由 View Manager 管理的完整虚拟机允许同时发生的电源操作（启动、关闭、挂起等）的最大数量。默认值为 5。此设置控制完整虚拟机和链接克隆虚拟机的电源操作。

10 选择是否配置 View Composer。

选项	操作
您未使用 View Composer	单击 **[OK（确定）]**。
您正在使用 View Composer	配置 View Composer 设置。

下一步

如果此 View Connection Server 实例或副本 View Connection Server 实例组使用多个 vCenter Server 实例，请重复此过程添加其他 vCenter Server 实例。

从 View Manager 中移除 vCenter Server 实例

您可以移除 View Manager 与 vCenter Server 实例之间的连接。移除后，View Manager 将不再管理由该 vCenter Server 实例创建的 View 桌面。

前提条件

删除所有与 vCenter Server 实例关联的 View 桌面。请参阅第 165 页，“从 View Manager 中删除桌面池”。

步骤

1 单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 在 [vCenter Server] 面板中，选择 vCenter Server 实例。

3 单击 **[Remove（移除）]**。

   这时将出现一个对话框，警告您 View Manager 将不能再访问由此 vCenter Server 实例管理的虚拟机。

4 单击 **[OK（确定）]**。

View Manager 无法再访问在 vCenter Server 实例中创建的虚拟机。

为 View Composer 创建用户帐户

如果您使用 View Composer，则必须在 Active Directory 中创建一个在 View Composer 中使用的用户帐户。View Composer 需要使用该帐户将链接克隆桌面加入 Active Directory 域。

为确保安全性，您应当创建一个单独的用户帐户供 View Composer 使用。通过创建单独的帐户，可以保证该帐户不具有针对其他用途定义的额外特权。您可以为该帐户授予在指定的 Active Directory 容器中创建和移除计算机对象所需的最低特权。例如，View Composer 帐户不需要域管理员特权。

步骤

1 在 Active Directory 中，在 View Connection Server 主机所在的域或受信任的域中创建一个用户帐户。

2 在创建链接克隆计算机帐户或链接克隆计算机帐户移至的 Active Directory 容器中，将 **[Create Computer Objects（创建计算机对象）]**、**[Delete Computer Objects（删除计算机对象）]** 和 **[Write All Properties（写入全部属性）]** 权限添加到该容器中的帐户。

   以下列表列出了该用户帐户所需的所有权限，包括默认分配的权限。

   - List Contents（列出内容）
   - Read All Properties（读取全部属性）
   - Write All Properties（写入全部属性）
   - Read Permissions（读取权限）
   - Create Computer Objects（创建计算机对象）
   - Delete Computer Objects（删除计算机对象）

3 确保用户帐户权限可应用于 Active Directory 容器以及该容器的所有子对象。

下一步

当您为 vCenter Server 配置 View Composer，以及配置和部署链接克隆桌面池时，需要在 View Administrator 中指定该帐户。

为 vCenter Server 配置 View Composer 设置

要使用 View Composer，您必须对 View Manager 进行配置，使其初始设置与 vCenter Server 上安装的 View Composer 服务的设置相匹配。View Composer 是 View Manager 的一项功能，但其服务直接在 vCenter Server 中虚拟机上运行。

注意 如果您不使用 View Composer，则可以跳过此任务。

前提条件

- 确认您在 Active Directory 中创建了一个有权从您的链接克隆所在 Active Directory 域添加或移除虚拟机的用户。请参阅第 13 页，“为 View Composer 创建用户帐户”。
- 确认您已将 View Manager 配置为连接到 vCenter Server。请参阅第 12 页，“将 vCenter Server 实例添加到 View Manager”。

步骤

1 在 View Administrator 中，打开 [Edit vCenter Server（编辑 vCenter Server）] 对话框。

   a 单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

   b 在 [vCenter Server] 面板中，选择 vCenter Server 条目。

   c 单击 **[Edit（编辑）]**。

2 选择 **[Enable View Composer（启用 View Composer）]** 并确保端口号与您在 vCenter Server 上安装 View Composer 服务时指定的端口号相一致。

   View Manager 会验证 View Composer 服务是否正在 vCenter Server 上运行。

3 单击 **[Add（添加）]** 以添加 View Composer 帐户信息中的域用户。

   a 键入 Active Directory 域的域名。

      例如：**`domain.com`**

   b 键入域用户名，包括域名。

      例如：**`domain.com\admin`**

   c 键入该帐户的密码。

   d 单击 **[OK（确定）]**。

   e 要添加在您部署链接克隆池的其他 Active Directory 域中具有特权的域用户帐户，请重复上述步骤。

4 单击 **[OK（确定）]** 关闭 [Edit vCenter Server（编辑 vCenter Server）] 对话框。

下一步

对安装了 View Composer 服务的每个 vCenter Server 实例重复此过程。

从 View Manager 中移除 View Composer

您可以移除 View Manager 与 vCenter Server 实例中安装的 View Composer 服务之间的连接。移除后，View Manager 将不再管理由该 vCenter Server 实例中的 View Composer 创建的链接克隆桌面。

在您禁用与 View Composer 的连接之前，必须先从 View Manager 中移除所有由 View Composer 创建的链接克隆桌面。禁用与 View Composer 的连接之后，View Manager 将无法部署、管理或删除链接克隆。View Manager 不会强制要求您删除链接克隆。您必须亲自执行该操作。

步骤

1 移除由 View Composer 创建的链接克隆池。

   a 在 View Administrator 中，单击 **[Inventory（清单）]** > **[Pools（池）]**。

   b 选择链接克隆池并单击 **[Delete（删除）]**。

      这时将出现一个对话框，警告您将从 View Manager 中永久删除链接克隆池。随后将从 vCenter Server 中删除虚拟机。此外，还会移除相关的 View Composer 数据库条目以及由 View Composer 创建的副本。

   c 单击 **[OK（确定）]**。

   d 对于由 View Composer 创建的每个链接克隆池，均重复上述步骤。

2 单击 **[View Configuration（View 配置）]** > **[Servers（服务器）]**。

3 在 [vCenter Server] 面板中，选择安装了 View Composer 的 vCenter Server 实例。

4 单击 **[Edit（编辑）]**。

5 在 [View Composer Settings（View Composer 设置）] 面板中，取消选中 **[Enable View Composer（启用 View Composer）]** 并单击 **[OK（确定）]**。

您将无法再在此 vCenter Server 实例中创建链接克隆桌面，但您可以继续在 vCenter Server 实例中创建及管理完整虚拟机桌面池。

在您禁用与 View Composer 的连接之前，如果没有删除链接克隆桌面，您可以尝试重新启用与 View Composer 的连接、删除链接克隆，然后再禁用与 View Composer 的连接。有关启用 View Composer 的详细信息，请参阅第 14 页，“为 vCenter Server 配置 View Composer 设置”。

vCenter Server 唯一 ID 冲突

如果在您的环境中配置了多个 vCenter Server 实例，添加新实例时可能会因为唯一 ID 冲突而失败。

问题

您试图在 View Manager 中添加一个 vCenter Server 实例，但是新 vCenter Server 实例的唯一 ID 与已有实例的 ID 冲突。

原因

两个 vCenter Server 实例不能使用相同的唯一 ID，默认情况下，vCenter Server 唯一 ID 是随机生成的，但您可以对它进行编辑。

解决方案

1 在 vSphere Client 中，单击 **[Administration（系统管理）] > [vCenter Server Settings（vCenter Server 设置）] > [Runtime Settings（运行时设置）]**。

2 键入一个新的唯一 ID，然后单击 **[OK（确定）]**。

有关编辑 vCenter Server 唯一 ID 值的详细信息，请参阅 vSphere 文档。

备份 View Connection Server

完成对 View Connection Server 的初始配置后，您应当计划对 View Manager 和 View Composer 配置数据进行定期备份。

有关备份和恢复 View 配置的信息，请参阅第 239 页，“备份和还原 View 配置数据”。

配置客户端会话设置

您可以配置全局设置，以便影响由 View Connection Server 实例或副本组管理的客户端会话。您可以设置会话超时长度，在客户端连接和 View Administrator 中要求使用 SSL，显示登录前消息和警告消息，以及设置其他客户端连接选项。

设置客户端会话和连接选项

您可以配置全局设置，以确定客户端会话和连接的工作方式。

全局设置并不专门针对某一个 View Connection Server 实例。它们会影响由独立的 View Connection Server 实例或副本实例组管理的所有客户端会话。

您也可以对 View Connection Server 实例进行配置，使其在 View 客户端与 View 桌面之间使用直接的非安全加密链路连接。有关配置直接连接的信息，请参阅第 18 页，“配置安全加密链路连接”。

前提条件

熟悉全局设置。请参阅第 17 页，“客户端会话和连接的全局设置”。

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Global Settings（全局设置）]**。

2 单击 **[Edit（编辑）]**。

3 配置全局设置。

4 单击 **[OK（确定）]**。

下一步

如果您更改了以下全局设置之一，则必须重新启动 View Connection Server 服务，所做更改才能生效。

- **Require SSL for client connections and View Administrator（需要将 SSL 用于客户端连接和 View Administrator）**
- **Reauthenticate secure VPN connections after network interruption（网络中断后对安全的 VPN 连接重新进行身份验证）**
- **Display a pre-login message（显示登录前的消息）**

在副本 View Connection Server 实例组中，您必须在组中的所有实例上重新启动 View Connection Server 服务。您不必重新启动安装了 View Connection Server 的 Windows Server 计算机。

客户端会话和连接的全局设置

全局设置可确定会话超时长度、是否使用 SSL、客户端在中断后是否要重新进行身份验证、View 组件是否使用安全的内部通信、是否显示登录前消息和警告消息，以及是否为本地桌面操作使用 SSO。

表 1–2 客户端会话和连接的全局设置

设置	描述
Session timeout（会话超时）	确定在用户登录 View Connection Server 后，能够将会话保持多长时间。 此值的单位为分钟。您必须键入一个值。默认值是 600 分钟。
Require SSL for client connections and View Administrator（需要将 SSL 用于客户端连接和 View Administrator）	确定 View Connection Server 和 View 桌面客户端之间，以及 View Connection Server 和访问 View Administrator 的客户端之间是否使用安全的 SSL 通信通道。 选择此设置时，客户端必须使用 SSL 连接。 如果使用智能卡身份验证则必须选择此设置。 更改此设置后，必须重新启动 View Connection Server 服务，才能使所做的更改生效。
Reauthenticate secure VPN connections after network interruption（网络中断后对安全的 VPN 连接重新进行身份验证）	如果您对客户端使用提供安全加密链路的安全 VPN 连接，则可以确定在网络中断后是否必须重新对用户凭据进行身份验证。 当您使用直接连接时，此设置无效。 更改此设置后，必须重新启动 View Connection Server 服务，才能使所做的更改生效。
Message security mode（消息安全模式）	确定 View Manager 组件之间的通信安全性。特别会确定是否对 View Manager 组件之间传输的 JMS 消息进行签发和验证。有关详细信息，请参阅第 18 页，“View 组件的消息安全模式”。
Disable Single Sign-On for Local Mode operations（对本地模式操作禁用单点登录）	确定在用户登录本地桌面时是否启用单点登录。 如果您禁用此设置，用户就必须手动登录桌面，才能在登录后启动其 Windows 会话。 当您更改此设置后，所做的更改会在每个用户下次操作时生效。
Enable automatic status updates（启用自动状态更新）	确定 View Manager 是否每隔几分钟便更新 View Administrator 左上角的全局状态窗格。View Administrator 的仪表板页面也会每隔几分钟更新一次。 启用此设置后，已登录 View Administrator 的任何用户的空闲会话都不会超时。 **重要事项** 禁用空闲会话超时会增加未经授权便使用 View Administrator 的风险。启用 此设置前请慎重考虑。 默认情况下不启用此设置，以免出现空闲会话超时问题。

表 1–2 客户端会话和连接的全局设置（续）

设置	描述
Display a pre-login message（显示登录前的消息）	在 View Client 用户登录时，对其显示免责声明或其他消息。 在 [Global Settings（全局设置）] 对话框窗口的文本框中键入您的信息或说明。 如果不希望显示任何消息，请将该文本框保留为空。 更改此设置后，必须重新启动 View Connection Server 服务，才能使所做的更改生效。
Display warning before forced logoff（强制注销前显示警告）	当用户因为计划更新或即时更新（如要开始桌面刷新操作）被强制注销时，显示一条警告信息。此设置还可确定从显示警告到注销用户之间的时间间隔。 选中该框可显示警告消息。 键入从显示警告到注销用户之间的分钟数。默认值是 5 分钟。 键入您的警告消息。您可以使用默认的消息： `Your desktop is scheduled for an important update and will be restarted in 5 minutes.Please save any unsaved work now.`（您的桌面需按计划执行一个重要更新，将在 5 分钟内重新启动。请立即保存尚未保存的工作。）

View 组件的消息安全模式

您可以为 View 组件之间的通信设置安全级别。此设置可确定是否签发和验证在 View Manager 组件之间传输的 JMS 消息。启用此设置可防止处理来自未经授权源的控制消息。

如果 View 环境中的任何组件早于 View Manager 3.0 版，则无法进行签发和验证。

表 1–3 显示了您可以选择用来配置消息安全级别的选项。要设置某个选项，请从 [Global Settings（全局设置）] 对话框窗口中的 **[Message security mode（消息安全模式）]** 列表中选择所需选项。

表 1–3 消息安全模式选项

选项	描述
Disabled（禁用）	禁用消息安全模式。
Mixed（混合）	启用消息安全模式，但并非强制使用。 您可以使用此模式来检测 View 环境中版本低于 View Manager 3.0 的组件。View Connection Server 生成的日志文件包含这些组件的相关信息。
Enabled（启用）	启用消息安全模式。未签名的消息会被 View 组件拒绝。 **注意** View Manager 3.0 之前的 View 组件 不可与其他 View 组件通信。

View Manager 3.1 和更高版本可支持消息安全模式。如果将消息安全模式由 **[Disabled（禁用）]** 或 **[Mixed（混合）]** 更改为 **[Enabled（启用）]**，您将无法通过 Virtual Desktop Manager 2.1 或更低版本启动具有 View Agent 的桌面。即使您随后将消息安全模式从 **[Enabled（启用）]** 更改为 **[Mixed（混合）]** 或 **[Disabled（禁用）]**，桌面也无法启动。要在将消息安全模式从 **[Enabled（启用）]** 更改为 **[Mixed（混合）]** 或 **[Disabled（禁用）]** 后启动桌面，您必须重新启动桌面。

配置安全加密链路连接

启用安全加密链路连接后，当用户使用 Microsoft RDP 显示协议连接至 View 桌面时，View Client 会和 View Connection Server 或安全服务器主机建立第二个 HTTPS 连接。

禁用安全加密链路连接后，View 桌面会话将绕过 View Connection Server 或安全服务器主机，直接在客户端系统和 View 桌面虚拟机之间建立。这种连接称为直接连接。

注意 使用 PCoIP 和 HP RGS 显示协议的客户端不使用安全加密链路连接。

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 在 View Connection Server 面板中，选择所需的 View Connection Server 实例，然后单击 **[Edit（编辑）]**。

选项	描述
禁用安全加密链路连接	取消选中 **[Use secure tunnel connection to desktop（使用安全加密链路连接桌面）]**。
启用安全加密链路连接	选择 **[Use secure tunnel connection to desktop（使用安全加密链路连接桌面）]**。

默认情况下安全加密链路连接处于启用状态。

3 单击 **[OK（确定）]** 保存更改。

禁用或启用 View Connection Server

您可以禁用 View Connection Server 实例，以禁止用户登录其 View 桌面。禁用实例后，可以重新启用。

禁用某个 View Connection Server 实例时，当前已登录 View 桌面的用户不会受到影响。

您的 View Manager 部署可确定禁用实例对用户产生的影响。

- 如果是独立的 View Connection Server 实例，用户就无法登录其桌面。他们无法连接到 View Connection Server。
- 如果是 View Connection Server 副本实例，那么您的网络拓扑结构将确定用户是否可以路由到另一个副本实例。如果用户可以访问另一个实例，他们就可以登录其桌面。

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 在 View Connection Server 面板中选择 View Connection Server 实例。

3 单击 **[Disable（禁用）]**。

您可以通过单击 **[Enable（启用）]** 再次启用该实例。

编辑外部 URL

您可以使用 View Administrator 编辑 View Connection Server 实例和安全服务器的外部 URL。

默认情况下，仅位于同一网络且使用安全加密链路的客户端可以联络 View Connection Server 或安全服务器主机。在您的网络外部运行的安全加密链路客户端必须使用可外部解析的 URL，才能连接到 View Connection Server 实例。

注意 您无法编辑尚未升级到 View Connection Server 4.5 的安全服务器的外部 URL。

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

选项	操作
View Connection Server 实例	在 View Connection Server 面板中选择 View Connection Server 实例并单击 **[Edit（编辑）]**。
安全服务器	在 Security Server 面板中选择安全服务器并单击 **[Edit（编辑）]**。

2 在 **[External URL（外部 URL）]** 文本框中键入外部 URL。

该 URL 必须包含协议、可外部解析的主机名和端口号。

例如：https://view.example.com:443

3 单击 **[OK（确定）]** 保存更改。

外部 URL 将立即更新。无需重新启动 View Connection Server 服务或安全服务器服务，所做更改即可生效。

View LDAP 目录

View LDAP 是所有 View Manager 配置信息的数据存储库。View LDAP 是一种嵌入式轻型目录访问协议 (Lightweight Directory Access Protocol, LDAP) 目录，它与 View Connection Server 安装程序一起提供。

View LDAP 包含 View Manager 所使用的标准 LDAP 目录组件。

- View Manager 模式定义
- 目录信息树 (DIT) 定义
- 访问控制列表 (ACL)

View LDAP 包含了表示 View Manager 对象的目录条目。

- View 桌面条目，表示每个可访问的桌面。每个条目均包含对 Active Directory 中有权使用此桌面的 Windows 用户和用户组的外部安全主体 (Foreign Security Principal, FSP) 条目的引用。
- View 桌面池条目，表示被集中管理的多个桌面
- 虚拟机条目，表示每个桌面的 vCenter Server 虚拟机
- View Manager 组件条目，用于存储配置设置

此外，View LDAP 还包含一整套 View Manager 插件 DLL，可为其他 View Manager 组件提供自动化服务和通知服务。

注意 安全服务器实例不包含 View LDAP 目录。

配置 View Connection Server 设置

您可以使用 View Administrator 来修改 View Connection Server 实例的配置设置。

配置基于角色的委托管理 2

View 环境中的一项关键管理任务是确定哪些用户能够使用 View Administrator，以及这些用户有执行哪些任务的权限。通过基于角色的委托管理，您可以将管理员角色分配给特定 Active Directory 用户和组，从而选择性地分配管理权限。

本章讨论了以下主题：

了解角色和特权

View Administrator 中的任务执行由一个访问控制系统管理，该系统由管理员角色和特权组成。该系统类似于 vCenter Server 访问控制系统。

管理员角色就是一组特权的集合。特权可授予执行特定操作的能力，例如授予用户对桌面池的权限。特权还控制管理员可在 View Administrator 中查看的内容。例如，如果某个管理员不具有查看或修改全局策略的特权，那么该管理员登录 View Administrator 时将看不到导航面板中的 **[Global Policies（全局策略）]** 设置。

管理员特权可以针对全局或特定对象。全局特权控制整个系统的操作，例如查看和更改全局设置。针对特定对象的特权可控制在特定清单对象类型上的操作。

管理员角色通常具有执行较高级别管理任务所需的各种特权。View Administrator 中包含的预定义角色具有执行常规管理任务所需的特权。您可以将这些预定义角色分配给管理员用户和用户组，也可以通过组合特定特权来自行创建角色。您无法修改预定义角色。

要创建管理员，可以从 Active Directory 用户和组中选择用户和组并分配管理员角色。管理员通过其角色分配获取特权。您无法将特权直接分配给管理员。具有多个角色的管理员拥有这些角色中包含的所有特权。

使用文件夹委托管理

默认情况下，桌面池创建在根文件夹中，并在 View Administrator 中显示为 / 或 Root(/)。您可以在根文件夹下创建文件夹细分桌面池，然后将特定桌面池的管理权委托给不同的管理员。

桌面会从其所在的池继承文件夹。连接的永久磁盘从其桌面继承文件夹。您最多可以创建 100 个文件夹，包括根文件夹。

您需要针对文件夹为管理员分配角色，才能配置对该文件夹中资源的管理员访问权限。管理员只能访问为其分配了相应角色文件夹中的资源。管理员在文件夹上的角色决定了其对该文件夹中资源所具有的访问权限级别。

由于角色可从根文件夹继承而来，因此在根文件夹上具有某个角色的管理员在所有文件夹上都具有该角色。在根文件夹上具有 Administrators 角色的管理员是超级管理员，因为他们对于系统中的所有清单对象具有完全访问权限。

角色中必须至少包含一个特定于对象的特权才能应用于文件夹。只包含全局特权的角色不能应用于文件夹。

您可以使用 View Administrator 创建文件夹，并将现有池移到文件夹中。您还可以在创建桌面池时选择文件夹。如果您在创建池时不选择文件夹，默认情况下池将被创建在根文件夹中。

- 为不同文件夹配置不同的管理员第 22 页，

  您可以创建不同的管理员来管理配置中的每个文件夹。

- 为同一文件夹配置不同管理员第 22 页，

  您可以创建不同的管理员来管理同一文件夹。

为不同文件夹配置不同的管理员

您可以创建不同的管理员来管理配置中的每个文件夹。

例如，如果您的企业桌面池位于一个文件夹中，而软件开发人员的专用桌面池位于另一个文件夹中，那么您可以创建不同的管理员来管理每个文件夹中的资源。

表 2‑1 显示了这种配置的示例。

表 2‑1 为不同文件夹配置不同的管理员

管理员	角色	文件夹
view-domain.com\Admin1	Inventory Administrators	/CorporateDesktops
view-domain.com\Admin2	Inventory Administrators	/DeveloperDesktops

在此示例中，名为 Admin1 的管理员在名为 CorporateDesktops 的文件夹中具有 Inventory Administrators 角色，名为 Admin2 的管理员在名为 DeveloperDesktops 的文件夹上具有 Inventory Administrators 角色。

为同一文件夹配置不同管理员

您可以创建不同的管理员来管理同一文件夹。

例如，如果您的企业桌面池位于一个文件夹中，您可以创建一个可以查看和修改这些池的管理员，另外再创建一个仅可查看这些池的管理员。

表 2‑2 显示了这种配置的示例。

表 2–2 为同一文件夹配置不同管理员

管理员	角色	文件夹
view-domain.com\Admin1	Inventory Administrators	/CorporateDesktops
view-domain.com\Admin2	Inventory Administrators (Read only)	/CorporateDesktops

在此示例中，名为 Admin1 的管理员在名为 CorporateDesktops 的文件夹上具有 Inventory Administrators 角色，名为 Admin2 的管理员在同一文件夹上具有 Inventory Administrators (Read only) 角色。

了解权限

View Administrator 中的角色、管理员用户或组以及文件夹的组合即为权限。角色定义了可以执行的操作，用户或组指明了谁可以执行操作，文件夹则包含操作的目标对象。

根据您选择的是管理员用户或组、文件夹或是角色，View Administrator 中将显示不同的权限。

表 2–3 显示了当您选择管理员用户或组时，权限在 View Administrator 中的显示方式。管理员用户名为 Admin 1，具有两个权限。

表 2–3 [Administrators and Groups（管理员和组）] 选项卡上显示的 Admin 1 权限

角色	文件夹
Inventory Administrators	MarketingDesktops
Administrators (Read only)	/

第一个权限表示 Admin 1 在名为 MarketingDesktops 的文件夹上具有 Inventory Administrators 角色。第二个权限表示 Admin 1 在根文件夹上具有 Administrators (Read only) 角色。

表 2–4 显示了当您选择 MarketingDesktops 文件夹时，View Administrator 中如何显示同样的权限。

表 2–4 [Folders（文件夹）] 选项卡上显示的 MarketingDesktops 权限

管理员	角色	是否为继承
view-domain.com\Admin1	Inventory Administrators	
view-domain.com\Admin1	Administrators (Read Only)	是

第一个权限与表 2–3 中显示的第一个权限相同。第二个权限是从表 2–3 中显示的第二个权限继承而来。由于文件夹从根文件夹继承权限，因此 Admin1 在 MarketingDesktops 文件夹上具有 Administrators (Read Only) 角色。如果权限是继承而来，那么 [Inherited（是否为继承）] 列中就会显示 [Yes（是）]。

表 2–5 表明当您选择 Inventory Administrators 角色时，View Administrator 如何显示表 2–3 中的第一个权限。

表 2–5 [Role（角色）] 选项卡上显示的 Inventory Administrators（清单管理员） 权限

管理员	文件夹
view-domain.com\Admin1	/MarketingDesktops

对管理员进行管理

具有 Administrators 角色的用户可以使用 View Administrator 来添加和移除管理员用户和组。

Administrators 角色是 View Administrator 中权限最高的角色。最初，View Connection Server 主机上的本地管理员组 (BUILTIN\Administrators) 成员会被授予 View Administrator 的 Administrators 角色。

注意 默认情况下，Domain Admins（域管理员）组是本地管理员组的成员。如果您希望域管理员可以完全访问清单对象和 View 配置设置，必须从本地管理员组移除 Domain Admins（域管理员）组。

- 创建管理员第 24 页，

  要创建管理员，您需要在 View Administrator 中从 Active Directory 用户和用户组内选择一个用户或用户组，然后分配管理员角色。

- 移除管理员第 25 页，

  您可以移除管理员用户或组，但无法移除系统中的最后一个超级管理员。超级管理员是在根目录上具有 Administrators 角色的管理员。

创建管理员

要创建管理员，您需要在 View Administrator 中从 Active Directory 用户和用户组内选择一个用户或用户组，然后分配管理员角色。

前提条件

- 熟悉预定义的管理员角色。请参阅第 30 页，“预定义的角色和特权”。
- 熟悉创建管理员用户和组的最佳实践。请参阅第 35 页，“针对管理员用户和组的最佳实践”。
- 如果要为管理员分配自定义角色，请创建自定义角色。请参阅第 29 页，“添加自定义角色”。
- 要创建可以管理特定桌面池的管理员，请创建一个文件夹并将桌面池移到该文件夹中。请参阅第 27 页，“管理和查看文件夹”。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Administrators（管理员）]**。

2 在 **[Administrators and Groups（管理员和组）]** 选项卡中，单击 **[Add User or Group（添加用户或用户组）]**。

3 单击 **[Add（添加）]**，选择一个或多个搜索条件，然后单击 **[Find（查找）]**，根据您的搜索条件来筛选 Active Directory 用户或用户组。

4 选择您希望将其设为管理员用户或组的 Active Directory 用户或用户组，然后依次单击 **[OK（确定）]** 和 **[Next（下一步）]**。

  您可以按 Ctrl 和 Shift 键来选择多个用户和用户组。

5 选择一个要分配给管理员用户或用户组的角色。

  [Apply to Folder（是否应用于文件夹）] 列表示角色是否应用于文件夹。只有包含特定于对象的特权的角色才可以应用于文件夹。只包含全局特权的角色不能应用于文件夹。

选项	操作
将您所选的角色应用于文件夹	选择一个或多个文件夹，然后单击 **[Next（下一步）]**。
您希望将该权限应用于所有文件夹	选择根文件夹，然后单击 **[Next（下一步）]**。

6 单击 **[Finish（完成）]** 创建管理员用户或组。

新的管理员用户或组将显示在 **[Administrators and Groups（管理员和组）]** 选项卡上的左侧窗格中，您选择的角色和文件夹显示在右侧窗格中。

移除管理员

您可以移除管理员用户或组，但无法移除系统中的最后一个超级管理员。超级管理员是在根目录上具有 Administrators 角色的管理员。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Administrators（管理员）]**。

2 在 **[Administrators and Groups（管理员和组）]** 选项卡上，选择所需的管理员或组，然后依次单击 **[Remove User or Group（移除用户或用户组）]** 和 **[OK（确定）]**。

[Administrators and Groups（管理员和组）] 选项卡上将不再显示该管理员用户或组。

管理和查看权限

您可以使用 View Administrator 来添加、删除和查看特定管理员用户和用户组、特定角色以及特定文件夹的权限。

- 添加权限第 26 页，
  您可以添加包含特定管理员用户或组、特定角色或特定文件夹的权限。
- 删除权限第 26 页，
  您可以删除包含特定管理员用户或组、特定角色或特定文件夹的权限。
- 查看权限第 27 页，
  您可以查看包含特定管理员或组、特定角色或特定文件夹的权限。

添加权限

您可以添加包含特定管理员用户或组、特定角色或特定文件夹的权限。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Administrators（管理员）]**。

2 创建权限。

选项	操作
创建包含特定管理员用户或组的权限	a 在 **[Administrators and Groups（管理员和组）]** 选项卡上，选择所需的管理员或组，然后单击 **[Add Permission（添加权限）]**。 b 选择一个角色。 c 如果该角色不能应用于文件夹，则单击 **[Finish（完成）]**。 d 如果该角色可应用于文件夹，则单击 **[Next（下一步）]**，选择一个或多个文件夹，然后单击 **[Finish（完成）]**。角色中必须至少包含一个特定于对象的特权才能应用于文件夹。
创建包含特定角色的权限	a 在 **[Roles（角色）]** 选项卡上，选择所需的角色，单击 **[Permissions（权限）]**，然后单击 **[Add Permission（添加权限）]**。 b 单击 **[Add（添加）]**，选择一个或多个搜索条件，然后单击 **[Find（查找）]** 来查找符合搜索条件的管理员用户或组。 c 选择要包含在权限中的管理员用户或组，然后单击 **[OK（确定）]**。您可以按 Ctrl 和 Shift 键来选择多个用户和用户组。 d 如果该角色不能应用于文件夹，则单击 **[Finish（完成）]**。 e 如果该角色可应用于文件夹，则单击 **[Next（下一步）]**，选择一个或多个文件夹，然后单击 **[Finish（完成）]**。角色中必须至少包含一个特定于对象的特权才能应用于文件夹。
创建包含特定文件夹的权限	a 在 **[Folders（文件夹）]** 选项卡上，选择所需的文件夹，然后单击 **[Add Permission（添加权限）]**。 b 单击 **[Add（添加）]**，选择一个或多个搜索条件，然后单击 **[Find（查找）]** 来查找符合搜索条件的管理员用户或组。 c 选择要包含在权限中的管理员用户或组，然后单击 **[OK（确定）]**。您可以按 Ctrl 和 Shift 键来选择多个用户和用户组。 d 单击 **[Next（下一步）]** 选择一个角色，然后单击 **[Finish（完成）]**。角色中必须至少包含一个特定于对象的特权才能应用于文件夹。

删除权限

您可以删除包含特定管理员用户或组、特定角色或特定文件夹的权限。

移除管理员用户或组的最后一个权限后，该管理员用户或组也随之被移除。由于必须至少有一个管理员在根文件夹上具有 Administrators 角色，因此如果移除某个权限会导致管理员被移除，您就不能移除该权限。您无法删除继承而来的权限。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Administrators（管理员）]**。

2 选择要删除的权限。

选项	操作
删除应用于特定管理员或组的权限	在 **[Administrators and Groups（管理员和组）]** 选项卡上选择管理员或组。
删除应用于特定角色的权限	在 **[Roles（角色）]** 选项卡上选择角色。
删除应用于特定文件夹的权限	在 **[Folders（文件夹）]** 选项卡上选择文件夹。

3 选择所需的权限，然后单击 **[Delete Permission（删除权限）]**。

查看权限

您可以查看包含特定管理员或组、特定角色或特定文件夹的权限。

步骤

1 选择 **[View Configuration（View 配置）] > [Administrators（管理员）]**。

2 查看权限。

选项	操作
查看包含特定管理员或组的权限	在 **[Administrators and Groups（管理员和组）]** 选项卡上选择管理员或组。
查看包含特定角色的权限	在 **[Roles（角色）]** 选项卡上选择角色，然后单击 **[Permissions（权限）]**。
查看包含特定文件夹的权限	在 **[Folders（文件夹）]** 选项卡上选择文件夹。

管理和查看文件夹

您可以使用 View Administrator 来添加和删除文件夹，以及查看特定文件夹中的桌面池和桌面。

■ 添加文件夹第 27 页，

如果您想将特定桌面或桌面池的管理权限委托给不同的管理员，则必须创建文件夹来细分桌面或桌面池。如果不创建文件夹，所有桌面和池都将驻留在根文件夹中。

■ 将桌面池移到不同的文件夹中第 28 页，

当您创建文件夹来细分桌面池时，您必须手动将桌面池移动到新文件夹中。如果决定更改桌面池的细分方式，您可以在文件夹之间移动桌面池。

■ 移除文件夹第 28 页，

当文件夹不包含清单对象时，您可以移除该文件夹。但您无法移除根文件夹。

■ 查看文件夹中的桌面池第 28 页，

您可以在 View Administrator 中查看特定文件夹中的所有桌面池。

■ 查看文件夹中的桌面第 29 页，

您可以在 View Administrator 中查看特定文件夹中的所有桌面。桌面会从其所在的池继承文件夹。

添加文件夹

如果您想将特定桌面或桌面池的管理权限委托给不同的管理员，则必须创建文件夹来细分桌面或桌面池。如果不创建文件夹，所有桌面和池都将驻留在根文件夹中。

您最多可以创建 100 个文件夹，包括根文件夹。

步骤

1 在 View Administrator 中，选择 **[Inventory（清单）]** > **[Pools（池）]**。

2 从命令栏的 **[Folder（文件夹）]** 下拉菜单中，选择 **[New Folder（新建文件夹）]**。

3 为文件夹键入名称和描述，然后单击 **[OK（确定）]**。

  描述是可选项。

下一步

将一个或多个桌面池移动到该文件夹中。

将桌面池移到不同的文件夹中

当您创建文件夹来细分桌面池时，您必须手动将桌面池移动到新文件夹中。如果决定更改桌面池的细分方式，您可以在文件夹之间移动桌面池。

步骤

1 在 View Administrator 中，选择 **[Inventory（清单）]** > **[Pools（池）]**，然后选择所需的池。

2 从 **[Folder（文件夹）]** 下拉菜单中，选择 **[Change Folder（更改文件夹）]**。

3 选择所需的文件夹，然后单击 **[OK（确定）]**。

View Administrator 会将该池移到选定的文件夹中。

移除文件夹

当文件夹不包含清单对象时，您可以移除该文件夹。但您无法移除根文件夹。

前提条件

如果文件夹包含清单对象，请将这些对象移动到另一个文件夹或根文件夹中。请参阅第 28 页，“将桌面池移到不同的文件夹中”。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）]** > **[Administrators（管理员）]**。

2 在 **[Folders（文件夹）]** 选项卡上，选择所需的文件夹，然后单击 **[Remove Folder（移除文件夹）]**。

3 单击 **[OK（确定）]** 移除文件夹。

查看文件夹中的桌面池

您可以在 View Administrator 中查看特定文件夹中的所有桌面池。

步骤

1 在 View Administrator 中，选择 **[Inventory（清单）]** > **[Pools（池）]**。

  [Pools（池）] 页面默认显示所有文件夹中的池。

2 从 **[Folder（文件夹）]** 下拉菜单中选择所需的文件夹。

  [Pools（池）] 页面将显示所选文件夹中的池。

查看文件夹中的桌面

您可以在 View Administrator 中查看特定文件夹中的所有桌面。桌面会从其所在的池继承文件夹。

步骤

1 在 View Administrator 中，选择 **[Inventory（清单）] > [Desktops（桌面）]**。

   [Desktops（桌面）] 页面默认显示所有文件夹中的桌面。

2 从 **[Folder（文件夹）]** 下拉菜单中选择所需的文件夹。

   [Desktops（桌面）] 页面将显示所选文件夹中的池。

管理自定义角色

您可以使用 View Administrator 来添加、修改和删除自定义角色。

- 添加自定义角色第 29 页，
  如果预定义的管理员角色不符合您的要求，您可以在 View Administrator 中组合特定特权以自行创建角色。
- 修改自定义角色中的特权第 29 页，
  您可以修改自定义角色中的特权，但无法修改预定义的管理员角色。
- 移除自定义角色第 30 页，
  如果自定义角色不包含在权限中时，您可以移除该角色，但您无法移除预定义的管理员角色。

添加自定义角色

如果预定义的管理员角色不符合您的要求，您可以在 View Administrator 中组合特定特权以自行创建角色。

前提条件

熟悉可用于创建自定义角色的管理员特权。请参阅第 30 页，“预定义的角色和特权”。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Administrators（管理员）]**。

2 在 **[Roles（角色）]** 选项卡上，单击 **[Add Role（添加角色）]**。

3 为新角色键入名称和描述，选择一个或多个特权，然后单击 **[OK（确定）]**。

   新角色将显示在左侧窗格中。

修改自定义角色中的特权

您可以修改自定义角色中的特权，但无法修改预定义的管理员角色。

前提条件

熟悉可用于创建自定义角色的管理员特权。请参阅第 30 页，“预定义的角色和特权”。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Administrators（管理员）]**。

2 在 **[Roles（角色）]**，选项卡上，选择所需的角色。

3 单击 **[Usage（使用情况）]** 显示该角色中的特权，然后单击 **[Edit（编辑）]**。

4 选择或取消选择特权。

5 单击 **[OK（确定）]** 保存更改。

移除自定义角色

如果自定义角色不包含在权限中时，您可以移除该角色，但您无法移除预定义的管理员角色。

前提条件

如果角色包含在权限中，请删除该权限。请参阅第 26 页，“删除权限”。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）]** > **[Administrators（管理员）]**。

2 在 **[Roles（角色）]** 选项卡上，选择所需的角色，然后单击 **[Remove Role（移除角色）]**。

   对于预定义角色或者包含在权限中的自定义角色，**[Remove Role（移除角色）]** 按钮不可用。

3 单击 **[OK（确定）]** 移除角色。

预定义的角色和特权

View Administrator 中包含预定义的角色，您可以将这些角色分配给管理员用户和组。您也可以组合特定的特权，自行创建管理员角色。

- 预定义的管理员角色第 30 页，

  预定义的管理员角色具有执行常见管理任务所需的所有特权。您无法修改预定义角色。
- 全局特权第 31 页，

  全局特权控制整个系统的操作，例如查看和更改全局设置。只包含全局特权的角色不能应用于文件夹。
- 特定于对象的特权第 32 页，

  针对特定对象的特权可控制在特定清单对象类型上的操作。包含对象专用特权的角色可以应用于文件夹。
- 内部特权第 33 页，

  某些预定义的管理员角色包含内部特权。您在创建自定义角色时无法选择内部特权。

预定义的管理员角色

预定义的管理员角色具有执行常见管理任务所需的所有特权。您无法修改预定义角色。

表 2-6 介绍了预定义角色，并指明了角色是否可以应用于文件夹。

表 2–6 View Administrator 中的预定义角色

角色	用户能力	是否应用于文件夹
Administrators	执行所有管理员操作，包括创建其他管理员用户和用户组。在根文件夹上具有 Administrators 角色的管理员是超级管理员，因为他们对于系统中的所有清单对象具有完全访问权限。由于 Administrators 角色包含所有特权，您应该将其分配给一组有限的用户。 最初，View Connection Server 主机上的本地 Administrators（管理员）组成员在根文件夹中被授予了此角色。 **重要事项** 管理员必须在根文件夹上具有 Administrators 角色才能执行以下任务： ■ 添加和删除文件夹。 ■ 在 View Administrator 中管理 ThinApp 应用程序和配置设置。 ■ 查看和修改 View Transfer Server 实例和 Transfer Server 存储库。 ■ 使用 `vdmadmin` 和 `vdmimport` 命令。	是
Administrators (Read only)	■ 查看但不能修改全局设置和清单对象。 ■ 查看但不能修改 ThinApp 应用程序和设置、View Transfer Server 实例和 Transfer Server 存储库。 ■ 使用 PowerShell 命令和命令行实用程序（包括 `vdmexport`，但 `vdmadmin` 和 `vdmimport` 除外）。 当管理员在文件夹上具有此角色时，只能查看该文件夹中的清单对象。	是
Agent Registration Administrators	注册未受管的桌面源（如物理系统、独立的虚拟机和终端服务器）。	否
Global Configuration and Policy Administrators	查看和修改全局策略与配置设置（针对管理员角色和权限的设置除外）、ThinApp 应用程序和设置、View Transfer Server 实例和 Transfer Server 存储库。	否
Global Configuration and Policy Administrators (Read only)	查看但不能修改全局策略与配置设置（针对管理员角色和权限的设置除外）、ThinApp 应用程序和设置、View Transfer Server 实例和 Transfer Server 存储库。	否
Inventory Administrators	■ 执行与桌面、会话和池相关的所有操作。 ■ 管理永久磁盘。 ■ 对链接克隆桌面进行重新同步、刷新和重新平衡，以及更改默认池映像。 当管理员在文件夹上具有此角色时，只能对该文件夹中的清单对象执行上述操作。	是
Inventory Administrators (Read only)	查看但不能修改清单对象。 当管理员在文件夹上具有此角色时，只能查看该文件夹中的清单对象。	是

全局特权

全局特权控制整个系统的操作，例如查看和更改全局设置。只包含全局特权的角色不能应用于文件夹。

表 2–7 介绍了全局特权，并列出了包含各个特权的预定义角色。

表 2–7 全局特权

特权	用户能力	预定义角色
Console Interaction（控制台交互）	登录和使用 View Administrator。	Administrators Administrators (Read only) Inventory Administrators Inventory Administrators (Read only) Global Configuration and Policy Administrators Global Configuration and Policy Administrators (Read only)
Direct Interaction（直接交互）	使用 PowerShell 命令和命令行实用程序（`vdmadmin` 和 `vdmimport` 除外）。 管理员必须在根文件夹上具有 Administrators 角色才能使用 `vdmadmin` 和 `vdmimport` 命令。	Administrators Administrators (Read only)
Manage Global Configuration and Policies（管理全局配置和策略）	查看和修改全局策略与配置设置（针对管理员角色和权限的设置除外）。	Administrators Global Configuration and Policy Administrators
Manage Roles and Permissions（管理角色和权限）	创建、修改和删除管理员角色和权限。	Administrators
Register Agent（注册 Agent）	在未受管的桌面源（如物理系统、独立的虚拟机和终端服务器）上安装 View Agent。 在 View Agent 安装过程中，您必须提供管理员登录凭据，才能在 View Connection Server 实例上注册未受管理的桌面源。	Administrators Agent Registration Administrators

特定于对象的特权

针对特定对象的特权可控制在特定清单对象类型上的操作。包含对象专用特权的角色可以应用于文件夹。

表 2–8 介绍了特定于对象的特权。预定义角色 Administrators 和 Inventory Administrators 中包含所有这些特权。

表 2–8 特定于对象的特权

特权	用户能力	对象
Enable Pool（启用池）	启用和禁用桌面池。	桌面池
Entitle Pool（授权池）	添加和移除用户授权。	桌面池
Manage Composer Pool Image（管理 Composer 池映像）	对链接克隆桌面进行重新同步、刷新和重新平衡，以及更改默认池映像。	桌面池
Manage Desktop（管理桌面）	执行与桌面和会话相关的所有操作。	桌面
Manage Local Sessions（管理本地会话）	回滚本地桌面和启动本地桌面复制。	桌面
Manage Persistent Disks（管理永久磁盘）	执行所有 View Composer 永久磁盘操作，包括附加、分离和导入永久磁盘。	永久磁盘
Manage Pool（管理池）	添加、修改和删除桌面池，以及添加和移除桌面。	桌面池
Manage Remote Sessions（管理远程会话）	断开连接并注销远程会话，并向桌面用户发送消息。	桌面
Manage Reboot Operation（管理重新启动操作）	重置桌面。	桌面

内部特权

某些预定义的管理员角色包含内部特权。您在创建自定义角色时无法选择内部特权。

表 2–9 介绍了内部特权，并列出了包含各个特权的预定义角色。

表 2–9 内部特权

特权	描述	预定义角色
Full (Read only)（完整（只读））	授予对所有设置的只读访问权限。	Administrators (Read only)
Manage Inventory (Read only)（管理清单（只读））	授予对清单对象的只读访问权限。	Inventory Administrators (Read only)
Manage Global Configuration and Policies (Read only)（管理全局配置和策略（只读））	授予只读访问配置设置和全局策略的权限，管理员和角色除外。	Global Configuration and Policy Administrators (Read only)

执行常见任务所需的特权

许多常见管理任务需要使用一组相互配合的特权。某些操作除需要访问操作对象的权限外，还需要访问根文件夹的权限。

管理池所需的特权

管理员必须具有某些特权才能在 View Administrator 中管理池。

表 2–10 列出了常见的池管理任务并显示了执行每个任务所需的特权。您可以在 View Administrator 的 [Pools（池）] 页面执行这些任务。

表 2–10 池管理任务和特权

任务	所需特权
启用或禁用池	**Enable Pool（启用池）** - 针对池。
将用户授权给池或取消授权	**Entitle Pool（授权池）** - 针对池。
添加池	**Manage Pool（管理池）** **重要事项** 添加链接克隆池时，您必须在根文件夹上具有 Administrators 角色才能将基础映像发布到 Transfer Server 存储库。
修改或删除池	**Manage Pool（管理池）** - 针对池。
从池添加或移除桌面	**Manage Pool（管理池）** - 针对池。
刷新、重构、重新平衡或更改默认的 View Composer 映像	**Manage Composer Pool Image（管理 Composer 池映像）** - 针对池。
更改文件夹	**Manage Pool（管理池）** — 针对源文件夹和目标文件夹。

管理桌面所需的特权

管理员必须具有某些特权才能在 View Administrator 中管理桌面。

表 2–11 中列出了常见的桌面管理任务并显示了执行每个任务所需的特权。您可在 View Administrator 的 [Desktops（桌面）] 页面执行这些任务。

表 2–11 桌面管理任务和特权

任务	所需特权
移除虚拟机	**Manage Pool（管理池）** - 针对池。
重置虚拟机	**Manage Reboot Operation（管理重新启动操作）** — 针对桌面。
取消、暂停或恢复任务	**Manage Composer Pool Image（管理 Composer 池映像）**
分配或移除用户所有权	**Manage Desktop（管理桌面）** — 针对桌面。
进入或退出维护模式	**Manage Desktop（管理桌面）** — 针对桌面。
回滚或启动复制	**Manage Local Sessions（管理本地会话）** — 针对桌面。
将远程会话断开连接或注销	**Manage Remote Sessions（管理远程会话）** — 针对桌面。

管理永久磁盘所需的特权

管理员必须具有某些特权才能在 View Administrator 中管理永久磁盘。

表 2–12 列出了常见的永久磁盘管理任务并显示了执行每个任务所需的特权。您需要在 View Administrator 的 [Persistent Disks（永久磁盘）] 页面执行这些任务。

表 2–12 永久磁盘管理任务和特权

任务	所需特权
分离磁盘	**Manage Persistent Disks（管理永久磁盘）** — 针对磁盘； **Manage Pool（管理池）** - 针对池。
附加磁盘	**Manage Persistent Disks（管理永久磁盘）** — 针对磁盘； **Manage Pool（管理池）** — 针对桌面。
编辑磁盘	**Manage Persistent Disks（管理永久磁盘）** — 针对磁盘； **Manage Pool（管理池）** — 针对所选的池。
更改文件夹	**Manage Persistent Disks（管理永久磁盘）** — 针对源文件夹和目标文件夹。
重新创建桌面	**Manage Persistent Disks（管理永久磁盘）** — 针对磁盘； **Manage Pool（管理池）** — 针对最后一个池。
从 vCenter 导入	**Manage Persistent Disks（管理永久磁盘）** — 针对文件夹； **Manage Pool（管理池）** - 针对池。
删除磁盘	**Manage Persistent Disks（管理永久磁盘）** - 针对磁盘。

管理用户和管理员所需的特权

管理员必须具有某些特权才能在 View Adminstrator 中管理用户和管理员。

表 2–13 列出了常见的用户和管理员管理任务并显示了执行每个任务所需的特权。您可在 View Administrator 的 [Users and Groups（用户和组）] 页面管理用户。您需要在 View Administrator 的 [Global Administrators View（全局管理员视图）] 页面管理管理员。

表 2–13 用户和管理员管理任务和特权

任务	所需特权
更新常规用户信息	**Manage Global Configuration and Policies（管理全局配置和策略）**
向桌面用户发送消息	**Manage Remote Sessions（管理远程会话）** — 针对桌面。
添加管理员用户或组	**Manage Roles and Permissions（管理角色和权限）**

表 2–13 用户和管理员管理任务和特权 （续）

任务	所需特权
添加、修改或删除管理员权限	**Manage Roles and Permissions（管理角色和权限）**
添加、修改或删除管理员角色	**Manage Roles and Permissions（管理角色和权限）**

执行常规管理任务和命令所需的特权

管理员必须具有某些特权才能执行常规管理任务和运行命令行实用程序。

表 2–14 显示了执行常规管理任务和运行命令行实用程序所需的特权。

表 2–14 执行常规管理任务和命令所需的特权

任务	所需特权
添加或删除文件夹	必须在根文件夹上具有 Administrators 角色。
在 View Administrator 中管理 ThinApp 应用程序和设置	必须在根文件夹上具有 Administrators 角色。
查看和修改 View Transfer Server 实例和 Transfer Server 存储库	必须在根文件夹上具有 Administrators 角色。
在未受管的桌面源（如物理系统、独立虚拟机或终端服务器）上安装 View Agent	**Register Agent（注册 Agent）**
查看或修改 View Administrator 中的配置设置（针对管理员的设置除外）	**Manage Global Configuration and Policies（管理全局配置和策略）**
使用 PowerShell 命令和命令行实用程序（`vdmadmin`、`vdmimport` 和 `vdmexport` 除外）	**Direct Interaction（直接交互）**
使用 `vdmadmin` 和 `vdmimport` 命令	必须在根文件夹上具有 Administrators 角色。
使用 `vdmexport` 命令	必须在根文件夹上具有 Administrators 角色或 Administrators (Read only) 角色。

针对管理员用户和组的最佳实践

要增加您的 View 环境的安全性和可管理性，在管理管理员用户和组时应该遵循以下最佳实践。

- 由于 Administrators 角色包含所有权限，因此请仅将该角色分配给单个用户或一组有限的用户。
- 选择一个本地 Windows 用户或组来为其分配 Administrators 角色。
- 为管理员创建新的用户组。避免使用 Windows 内置组或其他可能包含更多用户或组的现有组。
- 由于名称 Administrator 太过明显而且很容易猜到，因此在创建管理员用户和组时要避免使用该名称。
- 创建文件夹以隔离敏感桌面。将这些文件夹的管理委托给一组有限的用户。
- 创建可以修改全局策略和 View 配置设置的单独管理员。

准备未受管的桌面源 3

用户可以访问未受 vCenter Server 管理的机器所交付的 View 桌面。这些未受管的桌面源包括物理机、终端服务器以及在 VMware Server 和其他虚拟化平台上运行的虚拟机。您必须对未受管的桌面源进行准备，才能提供 View 桌面访问权限。

本章讨论了以下主题：

- 第 37 页，“为 View 桌面部署准备未受管的桌面源”
- 第 37 页，“在未受管的桌面源中安装 View Agent”

为 View 桌面部署准备未受管的桌面源

您必须执行特定任务来为 View 桌面部署准备未受管的桌面源。

前提条件

- 确认您拥有管理未受管桌面源的权限。
- 要确保将 View 桌面用户添加到未受管桌面源的本地 Remote Desktop Users（远程桌面用户）组，需要在 Active Directory 中创建一个受限制的 Remote Desktop Users（远程桌面用户）组。有关更多信息，请参阅 *《VMware View 安装指南》*。

步骤

1 开启未受管的桌面源并确认其可供 View Connection Server 实例访问。

2 将未受管的桌面源加入 View 桌面的 Active Directory 域。

3 将 Windows 防火墙配置为允许远程桌面连接到未受管的桌面源。

下一步

在未受管桌面源中安装 View Agent。请参阅第 37 页，“在未受管的桌面源中安装 View Agent”。

在未受管的桌面源中安装 View Agent

您必须在所有未受管的桌面源上安装 View Agent。如果不安装 View Agent，View 将无法管理未受管的桌面源。

要在多个 Windows 物理机上安装 View Agent，而又不想对向导提示作出响应，您可以静默安装 View Agent。请参阅第 47 页，“以静默方式安装 View Agent”。

前提条件

- 确认您拥有管理未受管桌面源的权限。
- 熟悉针对未受管桌面源的 View Agent 自定义安装选项。请参阅第 39 页，“针对未受管的桌面源的 View Agent 自定义安装选项”。

- 熟悉 View Agent 安装程序在防火墙上打开的 TCP 端口。有关更多信息，请参阅*《VMware View 体系结构规划指南》*。
- 从 VMware 产品页面下载 View Agent 安装程序文件，该页面的网址为：http://www.vmware.com/cn/products/。

步骤

1 要启动 View Agent 安装程序，请双击安装程序文件。

安装程序文件名为 `VMware-viewagent-4.5.0-`*`xxxxxx`*`.exe` 或 `VMware-viewagent-x86_64-4.5.0-`*`xxxxxx`*`.exe`，其中 *xxxxxx* 是内部版本号。

2 接受 VMware 许可条款。

3 选择自定义安装选项。

4 接受或更改目标文件夹。

5 在 **[Server（服务器）]** 文本框中，键入 View Connection Server 主机的主机名或 IP 地址。

在安装过程中，安装程序会在该 View Connection Server 实例上注册未受管的桌面源。注册后，指定的 View Connection Server 实例以及同一 View Connection Server 组中的任何其他实例，都可以与该未受管的桌面源进行通信。

6 选择一个身份验证方法以便在 View Connection Server 实例上注册未受管的桌面源。

选项	操作
Authenticate as the currently logged in user（作为当前登录的用户进行身份验证）	**[Username（用户名）]** 和 **[Password（密码）]** 文本框将被禁用，您将通过当前用户名和密码登录到 View Connection Server 实例。
Specify administrator credentials（指定管理员凭据）	您必须在 **[Username（用户名）]** 和 **[Password（密码）]** 文本框中提供 View Connection Server 管理员的用户名和密码。

7 按照 View Agent 安装程序中的提示完成安装。

8 如果您选择了 [USB redirection（USB 重定向）] 选项，则需要重新启动未受管的桌面源才能启用 USB 支持。

此外，**[Found New Hardware（发现新硬件）]** 向导也可能启动。在重新启动未受管的桌面源之前，请按照向导中的提示配置硬件。

VMware View Agent 服务将在未受管的桌面源上启动。

如果未安装 Windows Media Player，View Agent 安装程序不会安装多媒体重定向 (MMR) 功能。如果您在安装 View Agent 后安装 Windows Media Player，您可以通过再次运行 View Agent 安装程序，并选择 [Repair（修复）] 选项来安装 MMR 功能。

下一步

使用未受管的桌面源来创建 View 桌面。请参阅第 85 页，“手动桌面池”。

针对未受管的桌面源的 View Agent 自定义安装选项

在未受管的桌面源上安装 View Agent 时，您可以选择特定的自定义安装选项。

表 3–1 针对未受管的桌面源的 View Agent 自定义安装选项

选项	描述
USB Redirection（USB 重定向）	允许用户访问其桌面上本地连接的 USB 设备。 Windows 2000 不支持 USB 重定向。 **注意** 您可以使用组策略设置为特定用户禁用 USB 重定向。
PCoIP Server（PCoIP 服务器）	允许用户使用 PCoIP 显示协议连接至 View 桌面。 **注意** 在 Windows Vista 中，如果您安装了 PCoIP Server 组件，则 Windows 组策略 **[Disable or enable software Secure Attention Sequence（禁用或启用软件安全注意序列）]** 将启用，并设置为 **[Services（服务）]** 和 **[Ease of Access applications（轻松访问应用程序）]**。如果您更改此设置，单点登录功能将无法正常工作。
PCoIP 智能卡	允许用户在使用 PCoIP 显示协议时使用智能卡进行身份验证。 Windows Vista 不支持 PCoIP 智能卡子功能。

创建和准备虚拟机 4

您可以使用 vCenter Server 管理的虚拟机来部署 View 桌面。您可以将 vCenter Server 管理的虚拟机用作自动池的模板、链接克隆池的父虚拟机或者手动池中的桌面源。您必须对虚拟机进行适当准备，才能提供 View 桌面访问。

本章讨论了以下主题：

为 View 桌面部署创建虚拟机

最初的虚拟机会建立用于快速部署 View 桌面的虚拟硬件配置文件和操作系统。

1 为 View 桌面部署创建虚拟机第 42 页，

   您可以使用 vSphere Client 在 vCenter Server 中为 View 桌面创建虚拟机。

2 安装客户操作系统第 43 页，

   创建虚拟机后，必须安装客户操作系统。

3 为 View 桌面部署准备客户操作系统第 44 页，

   您必须执行某些特定任务来为 View 桌面部署准备客户操作系统。

为 View 桌面部署创建虚拟机

您可以使用 vSphere Client 在 vCenter Server 中为 View 桌面创建虚拟机。

前提条件

- 将客户操作系统中的一个 ISO 映像上传至 ESX Server 上的一个数据存储中。
- 熟悉虚拟机自定义配置参数。请参阅第 42 页，“虚拟机自定义配置参数”。

步骤

1 在 vSphere Client 中，登录到 vCenter Server 系统。

2 选择 **[File（文件）] > [New（新建）] > [Virtual Machine（虚拟机）]**，启动 [New Virtual Machine（新建虚拟机）] 向导。

3 选择 **[Custom（自定义）]**，配置自定义配置参数。

4 选择 **[Edit the virtual machine settings before completion（在完成之前编辑虚拟机设置）]**，然后单击 **[Continue（继续）]** 配置硬件设置。

   a 添加一个 CD/DVD 驱动器，设置媒体类型以使用 ISO 映像，选择您上传到数据存储中的客户操作系统 ISO 映像文件，然后选择 **[Connect at power on（开机时连接）]**。

   b 如果要安装 Windows XP 客户操作系统，请添加一个软盘驱动器，并将 **[Device Type（设备类型）]** 设置为 **[Client Device（客户端设备）]**。

   c 将 **[Power-on Boot Delay（开机引导延迟）]** 设置为 10,000 毫秒。

5 单击 **[Finish（完成）]** 以创建虚拟机。

下一步

在虚拟机上安装客户操作系统。

虚拟机自定义配置参数

为 View 桌面部署创建虚拟机时，您可以使用虚拟机自定义配置参数作为基准设置。

如果将 View Administrator 用作部署桌面池的 View 桌面管理器，则在部署基于模板的 View 桌面时可以更改这些设置。

表 4–1 自定义配置参数

参数	描述和建议
Name and Location（名称和位置）	虚拟机的名称和位置。 如果打算将该虚拟机用作模板，应当指定一个通用名称。位置可以是数据中心清单内的任意文件夹。
Host/Cluster（主机/群集）	将运行该虚拟机的 ESX Server 或服务器群集资源。 如果打算使用该虚拟机作为模板，则初始虚拟机的位置不必指定以后由模板创建的虚拟机将驻留的位置。
Resource pool（资源池）	如果物理 ESX Server 资源分为若干资源池，您可以将它们分配给虚拟机。
Datastore（数据存储）	与虚拟机关联的文件的位置。
Guest Operating System（客户操作系统）	在虚拟机中安装的操作系统的类型。
CPU	虚拟机中虚拟处理器的数目。 对于大多数客户操作系统来说，一个处理器已经足够。

表 4–1 自定义配置参数 （续）

参数	描述和建议
Memory（内存）	分配给虚拟机的内存容量。 在多数情况下，512 MB 已经足够。
Network（网络）	虚拟机中虚拟网络适配器 (NIC) 的数目。 通常情况下，一个 NIC 已经足够。虚拟基础架构的网络名称应当一致。如果模板中的网络名称错误，将导致实例自定义阶段失败。 在具有多个 NIC 的虚拟机上安装 View Agent 时，必须配置 View Agent 使用的子网。有关更多信息，请参见第 50 页，“为 View Agent 配置具有多个 NIC 的虚拟机”。
SCSI Controller（SCSI 控制器）	在虚拟机中使用的 SCSI 适配器类型。 在 Windows 7 和 Windows XP 客户操作系统中，您应该指定 LSI Logic 适配器。LSI Logic 适配器性能更佳，与通用 SCSI 设备协作效果更好。 LSI Logic SAS 仅在硬件版本为 7 的虚拟机中可用。 **注意** Windows XP 中不包含 LSI Logic 适配器驱动程序。您必须从 LSI Logic 网站下载驱动程序。
Select a Disk（选择磁盘）	要在虚拟机中使用的磁盘。 根据您决定分配给每个用户的本地存储容量，创建一个新的虚拟磁盘。应为操作系统安装程序、修补程序以及本地安装的应用程序提供足够的存储空间。 为降低磁盘空间和本地数据管理需求，您应当将用户的信息、配置文件和文档存储在网络共享位置，而不是本地磁盘。

安装客户操作系统

创建虚拟机后，必须安装客户操作系统。

前提条件

- 确认客户操作系统中的一个 ISO 映像位于 ESX Server 上的一个数据存储中。
- 确认虚拟机中的 CD/DVD 驱动器指向客户操作系统的 ISO 映像文件，并且配置为在开机时连接。
- 如果要安装 Windows XP，并为虚拟机选择了 LSI Logic 适配器，请从 LSI Logic 网站下载 LSI20320-R 控制器驱动程序，创建一个包含该驱动程序的软盘映像 (`.flp`) 文件，并将该文件上传到 ESX Server 上的数据存储。

步骤

1. 在 vSphere Client 中，登录到虚拟机所在的 vCenter Server 系统。
2. 右键单击虚拟机，选择 **[Power（电源）]**，然后选择 **[Power On（开机）]** 启动虚拟机。

   由于已将 CD/DVD 驱动器配置为指向客户操作系统 ISO 映像并在开机时连接，因此客户操作系统安装进程将自动开始。
3. 单击 **[Console（控制台）]** 选项卡，按照操作系统供应商提供的安装说明操作。

4 如果要安装 Windows XP 且已为虚拟机选择了 LSI Logic 适配器，请在 Windows 安装进程中安装 LSI Logic 驱动程序。

   a 按 F6 键可选择更多 SCSI 驱动程序。

   b 键入 S 可指定另一个设备。

   c 在 vSphere Client 工具栏中，单击 **[Connect Floppy（连接软盘）]**，选择 LSI Logic 驱动程序的软盘映像 (`.flp`) 文件。

   d 返回到 Windows Setup（Windows 安装程序）屏幕，按 Enter 键继续执行 Windows 安装进程。

   e 当 Windows 安装进程结束后，断开虚拟软盘驱动器的连接。

5 如果您正在安装 Windows 7，请在线激活 Windows。

下一步

为 View 桌面部署准备客户操作系统。

为 View 桌面部署准备客户操作系统

您必须执行某些特定任务来为 View 桌面部署准备客户操作系统。

前提条件

- 创建虚拟机并安装客户操作系统。
- 为 View 桌面配置一个 Active Directory 域控制器。有关更多信息，请参阅*《VMware View 安装指南》*。
- 确保将 View 桌面用户添加到虚拟机的本地 Remote Desktop Users 组中，在 Active Directory 中创建一个受限制的 Remote Desktop Users 组。有关更多信息，请参阅*《VMware View 安装指南》*。
- 确认您具有客户操作系统的管理权限。

步骤

1 在 vSphere Client 中，登录到虚拟机所在的 vCenter Server 系统。

2 右键单击虚拟机，选择 **[Power（电源）]**，然后选择 **[Power On（开机）]** 启动虚拟机。

3 右键单击虚拟机，选择 **[Guest（客户机）]**，然后选择 **[Install/Upgrade VMware Tools（安装/升级 VMware Tools）]**，以安装最新版本的 VMware Tools。

4 使用 VMware Tools 时间同步功能确保虚拟机与 ESX 同步。

   ESX 必须与一个内部 NTP 源同步，例如，与 Active Directory 相同的时间源。

   VMware Tools 联机帮助提供了配置客户机和主机时间同步的信息。

5 安装服务包和更新。

6 安装防病毒软件。

7 安装其他应用程序和软件，如 Windows Media Player（如果使用 MMR）和智能卡驱动程序（如果使用智能卡身份验证功能）。

   重要事项 如果要安装 Microsoft .NET Framework，您必须在安装 View Agent 后再安装此服务。

8 如果 View 客户端将通过 PCoIP 显示协议连接至虚拟机，请将电源选项 **[Turn off the display（关闭显示器）]** 设置为 **[Never（从不）]**。

   如果您不禁用此设置，当节能模式启动时，显示器会冻结在其最后的状态。

9 如果您的网络环境中使用了代理服务器，请配置网络代理设置。

10 配置网络连接属性。

  a 分配一个静态 IP 地址或指定一个由 DHCP 服务器分配的 IP 地址。

    View 不支持 View 桌面的链接克隆 (169.254.x.x) 地址。

  b 将首选及备用 DNS 服务器地址设置为您的 Active Directory 服务器地址。

11 将虚拟机加入 View 桌面的 Active Directory 域。

   您无需将 View Composer 使用的父虚拟机加入 Active Directory 域。父虚拟机可以是本地 WORKGROUP 的一员。

12 将 Windows 防火墙配置为允许远程桌面连接到虚拟机。

13 （可选）配置用户自定义脚本。

下一步

安装 View Agent 请参阅第 45 页，“在虚拟机中安装 View Agent”。

在虚拟机中安装 View Agent

您必须在由 vCenter Server 管理的虚拟机上安装 View Agent，View Connection Server 才能与这些虚拟机通信。在用作自动桌面池的模板、链接克隆桌面池的父虚拟机，以及手动桌面池的桌面源的所有虚拟机中安装 View Agent。

要在多个 Windows 虚拟机上安装 View Agent，而同时又不想响应向导提示，您可以静默安装 View Agent。请参阅第 47 页，“以静默方式安装 View Agent”。

前提条件

- 为 View 桌面部署准备客户操作系统。请参阅第 44 页，“为 View 桌面部署准备客户操作系统”。
- 从 VMware 产品页面下载 View Agent 安装程序文件，该页面的网址为：http://www.vmware.com/cn/products/。
- 确认您具有虚拟机的管理权限。
- 熟悉 View Agent 自定义安装选项。请参阅第 46 页，“View Agent 自定义安装选项”。
- 熟悉 View Agent 安装程序在防火墙上打开的 TCP 端口。有关更多信息，请参阅 *《VMware View 体系结构规划指南》*。
- 如果您选择 View Composer Agent 自定义安装选项，请确认您有使用 View Composer 的许可。

步骤

1 要启动 View Agent 安装程序，请双击安装程序文件。

  安装程序文件名为 `VMware-viewagent-4.5.0-`*`xxxxxx`*`.exe` 或 `VMware-viewagent-x86_64-4.5.0-`*`xxxxxx`*`.exe`，其中 *xxxxxx* 是内部版本号。

2 接受 VMware 许可条款。

3 选择自定义安装选项。

  要部署链接克隆桌面，请选择 **[View Composer Agent]** 选项。

4 接受或更改目标文件夹。

5 按照 View Agent 安装程序中的提示完成安装。

注意 如果您在准备客户操作系统的过程中没有启用远程桌面支持，View Agent 安装程序会提示您启用此功能。如果您在 View Agent 安装过程中没有启用远程桌面支持，安装完成后您必须手动启用此功能。

6 如果您选择了 [USB redirection（USB 重定向）] 选项，需要重新启动虚拟机以启用 USB 支持。

此外，**[Found New Hardware（发现新硬件）]** 向导也可能启动。在重新启动虚拟机之前，请先按照向导中的提示配置硬件。

虚拟机上会启动 VMware View Agent 服务。

如果您选择了 **[View Composer Agent]** 选项，虚拟机上将启动 VMware View Composer Guest Agent Server 服务。

如果未安装 Windows Media Player，View Agent 安装程序不会安装多媒体重定向 (MMR) 功能。如果您在安装 View Agent 后安装 Windows Media Player，您可以通过再次运行 View Agent 安装程序，并选择 [Repair（修复）] 选项来安装 MMR 功能。

下一步

如果虚拟机具有多个 NIC，则需要配置 View Agent 使用的子网。请参阅第 50 页，“为 View Agent 配置具有多个 NIC 的虚拟机”。

View Agent 自定义安装选项

在虚拟机上安装 View Agent 时，您可以选择自定义安装选项。

表 4–2 View Agent 自定义安装选项

选项	描述
USB Redirection（USB 重定向）	允许用户访问其桌面上本地连接的 USB 设备。 Windows 2000 不支持 USB 重定向。 **注意** 您可以使用组策略设置为特定用户禁用 USB 重定向。
View Composer Agent	允许在通过该虚拟机部署的链接克隆桌面上运行 View Agent。
Virtual Printing（虚拟打印）	允许用户通过其客户端计算机上可用的任意打印机进行打印。用户不需要在其桌面上另外安装驱动程序。
PCoIP Server	允许用户使用 PCoIP 显示协议连接至 View 桌面。 安装 PCoIP Server 功能会禁用 Windows 7 和 Windows Vista 桌面的睡眠模式以及 Windows XP 桌面的待机模式。当用户导航至 [Power Options（电源选项）] 或 [Shut Down（关机）] 菜单时，睡眠模式或待机模式是无效的。经过一段默认的非活动时间后，桌面不会进入睡眠或待机模式。桌面将一直处于活动模式。 **注意** 如果您在 Windows Vista 中安装了 PCoIP Server 功能，则 Windows 组策略 **[Disable or enable software Secure Attention Sequence（禁用或启用软件安全注意序列）]** 将启用，并设置为 **[Services（服务）]** 和 **[Ease of Access applications（轻松访问应用程序）]**。如果您更改此设置，单点登录功能将无法正常工作。
PCoIP 智能卡	允许用户在使用 PCoIP 显示协议时使用智能卡进行身份验证。 Windows Vista 不支持 PCoIP 智能卡子功能。

以静默方式安装 View Agent

您可以使用 Microsoft Windows Installer (MSI) 的静默安装功能，在若干 Windows 虚拟机或物理机上安装 View Agent。在静默安装过程中，您需要使用命令行，并且不必对向导提示作出响应。

利用静默安装功能，您可以在大型企业中高效部署 View 组件。

前提条件

- 为 View 桌面部署准备客户操作系统。请参阅第 44 页，“为 View 桌面部署准备客户操作系统”。
- 从 VMware 产品页面下载 View Agent 安装程序文件，该页面的网址为：http://www.vmware.com/cn/products/。

  安装程序文件名为 `VMware-viewagent-4.5.0-`*`xxxxxx`*`.exe` 或 `VMware-viewagent-x86_64-4.5.0-`*`xxxxxx`*`.exe`，其中 *xxxxxx* 是内部版本号。
- 确认您具有虚拟机或物理机的管理权限。
- 熟悉 View Agent 自定义安装选项。请参阅第 46 页，“View Agent 自定义安装选项”。
- 如果您选择 View Composer Agent 自定义安装选项，请确认您有使用 View Composer 的许可。
- 熟悉 MSI 安装程序的命令行选项。请参阅第 48 页，“Microsoft Windows Installer 命令行选项”。
- 熟悉 View Agent 中可用的静默安装属性。请参阅第 49 页，“View Agent 静默安装属性”。
- 熟悉 View Agent 安装程序在防火墙上打开的 TCP 端口。有关更多信息，请参阅《*VMware View 体系结构规划指南*》。

步骤

1. 在虚拟机或物理机上打开一个 Windows 命令提示符。
2. 在一行中键入安装命令。

   以下示例将在一个受 vCenter Server 管理的虚拟机中安装 View Agent。安装程序配置了 PCoIP、View Composer Agent、虚拟打印以及 USB 重定向等自定义安装选项。

   ```
   VMware-viewagent-4.5.0-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1
   ADDLOCAL=core,GINA,PCoIP,SVIAgent,ThinPrint,USB"
   ```

   以下示例将在一台不受管理的计算机上安装 View Agent，并通过指定的 View Connection Server `cs1.companydomain.com` 来注册桌面。安装程序配置了 SSO、虚拟打印以及 USB 重定向等自定义安装选项。

   ```
   VMware-viewagent-4.5.0-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=0
   VDM_SERVER_NAME=cs1.companydomain.com VDM_SERVER_USERNAME=admin.companydomain.com
   VDM_SERVER_PASSWORD=secret ADDLOCAL=core,GINA,ThinPrint,USB"
   ```

虚拟机上会启动 VMware View Agent 服务。

如果您选择了 **[View Composer Agent]** 选项，虚拟机上将启动 VMware View Composer Guest Agent Server 服务。

如果未安装 Windows Media Player，View Agent 安装程序不会安装多媒体重定向 (MMR) 功能。如果您在安装 View Agent 后安装 Windows Media Player，您可以通过再次运行 View Agent 安装程序，并选择 [Repair （修复）] 选项来安装 MMR 功能。

下一步

如果虚拟机具有多个 NIC，则需要配置 View Agent 使用的子网。请参阅第 50 页，“为 View Agent 配置具有多个 NIC 的虚拟机”。

Microsoft Windows Installer 命令行选项

要以静默方式安装 View 组件，必须使用 Microsoft Windows Installer (MSI) 命令行选项与属性。View 组件安装程序是 MSI 程序，采用标准的 MSI 功能。

有关 MSI 的详细信息，请参阅 Microsoft 网站。有关 MSI 命令行选项，请访问 Microsoft Developer Network (MSDN) Library 网站并搜索 MSI 命令行选项。要了解 MSI 命令行的用法，可以在安装了 View 组件的计算机上打开一个命令提示符，并键入 `msiexec /?`。

要以静默方式运行 View 组件安装程序，应当首先禁用引导程序，因为该程序会将安装程序提取到一个临时目录中，并启动交互式安装。

您必须在命令行输入控制安装程序引导程序的命令行选项。

表 4–3 View 组件引导程序的命令行选项

选项	描述
`/s`	禁用引导程序初始屏幕和提取对话框，从而阻止显示交互式对话。 例如：`VMware-viewconnectionserver-4.5.`*`x-xxxxxx`*`.exe /s` 运行静默安装时，必须使用 `/s` 选项。
`/v"` *`MSI 命令行选项`*`"`	指示安装程序传递您在命令行中作为一组选项输入的、括在双引号中的字符串，以便 MSI 进行解释。您必须将命令行输入项括在双引号中。应当在 `/v` 后面和命令行结尾处各输入一个双引号。 例如：`VMware-viewagent-4.5.`*`x-xxxxxx`*`.exe /s /v"`*命令行选项*`"` 要指示 MSI 安装程序解释包含空格的字符串，应当将该字符串括在两组双引号中。例如，您可能需要将 View 组件安装在名称中包含空格的安装路径下。 例如：`VMware-viewconnectionserver-4.5.`*`x-xxxxxx`*`.exe /s /v"`*命令行选项* `INSTALLDIR=""d:\abc\my folder"""` 在此示例中，MSI 安装程序会传递安装目录的路径，而不会试图将该字符串解释为两个命令行选项。请注意，最后一个双引号的作用是将整个命令行括住。 运行静默安装时，必须要使用 `/v"`*命令行选项*`"` 选项。

您可以通过将命令行选项和 MSI 属性值传递给 MSI 安装程序 `msiexec.exe`，来控制静默安装过程的提示。MSI 安装程序中包含 View 组件的安装代码。该程序将使用您在命令行中输入的值和选项来解释特定于 View 组件的安装选择和设置选项。

表 4–4 MSI 命令行选项和 MSI 属性

MSI 选项或属性	描述
`/qn`	指示 MSI 安装程序不显示安装程序向导页面。 例如，您可能希望采用默认的安装选项和功能，以静默方式安装 View Agent： `VMware-viewagent-4.5.`*`x-xxxxxx`*`.exe /s /v"/qn"` 或者，也可以使用 `/qb` 选项在非交互式自动安装中显示向导页面。随着安装的进行，向导页面会出现，但是您无法对其进行响应。 运行静默安装时，必须要使用 `/qn` 或 `/qb` 选项。
`INSTALLDIR`	指定 View 组件的备选安装路径。 采用 *`INSTALLDIR=路径`* 格式来指定安装路径。如果您要将 View 组件安装在默认路径下，则可以忽略此 MSI 属性。 此 MSI 属性是可选属性。

表 4–4 MSI 命令行选项和 MSI 属性（续）

MSI 选项或属性	描述
ADDLOCAL	确定要安装的特定于组件的功能。在交互式安装中，View 安装程序会显示自定义安装选项供您选择。利用 ADDLOCAL 这一 MSI 属性，您可以在命令行中指定这些安装选项。 要安装所有可选的自定义安装选项，请输入 ADDLOCAL=ALL。 例如：VMware-viewagent-4.5.*x-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" 如果您不使用 MSI 属性 ADDLOCAL，则程序将安装默认安装选项。 要单独指定各个安装选项，可输入以逗号分隔的安装选项名称列表。不要在名称之间输入空格。采用以下格式：*ADDLOCAL=值,值,值...*。 例如，您可能希望将 View Agent 连同 View Composer Agent 和 PCoIP 功能一起安装在客户操作系统中： VMware-viewagent-4.5.*x-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP" **注意** Core 功能是 View Agent 中必需的。 此 MSI 属性是可选属性。
/l*v *日志文件*	将日志信息写入具有详细输出的指定日志文件。 例如：/l*v ""%TEMP%\vmmsi.log"" 此示例会生成详细的日志文件，类似于在交互式安装过程中生成的日志文件。 可以利用此选项记录专门应用在您的安装中的自定义功能。您可以利用记录的信息在以后的静默安装中指定安装功能。 /l*v 选项是可选选项。

View Agent 静默安装属性

当您从命令行静默安装安全服务器时，可以加入某些特定的属性。必须采用 *属性=值* 格式，以便 Microsoft Windows Installer (MSI) 解释这些属性和值。

表 4–5 显示了可在命令行中使用的 View Agent 静默安装属性。

表 4–5 用于静默安装 View Agent 的 MSI 属性

MSI 属性	描述	默认值
INSTALLDIR	View Agent 软件的安装路径和文件夹。 例如：INSTALLDIR=""D:\abc\my folder"" 括住路径的两组双引号可允许 MSI 安装程序忽略路径中的空格。 此 MSI 属性是可选属性。	%ProgramFiles%\VMware, Inc.\VMware View Agent
RDPCHOICE	确定是否在桌面上启用远程桌面协议 (RDP)。 值为 1 时启用 RDP。值为 0 时禁用 RDP 设置。 此 MSI 属性是可选属性。	1
VDM_VC_MANAGED_AGENT	确定 vCenter Server 是否管理安装了 View Agent 的虚拟机。 值为 1 时将桌面配置为受 vCenter Server 管理的虚拟机。 值为 0 时将桌面配置为不受 vCenter Server 管理。 此 MSI 属性是必要属性。	无
VDM_SERVER_NAME	View Agent 安装程序在其中注册未受管桌面的 View Connection Server 计算机的主机名或 IP 地址。此属性适用于未受管的桌面。 例如：VDM_SERVER_NAME=10.123.01.01 此 MSI 属性是未受管桌面的必要属性。 不要将此 MSI 属性用于受 vCenter Server 管理的虚拟机桌面。	无

表 4–5 用于静默安装 View Agent 的 MSI 属性 （续）

MSI 属性	描述	默认值
VDM_SERVER_USERNAME	View Connection Server 计算机上的管理员用户名。此 MSI 属性适用于未受管的桌面。 例如：`VDM_SERVER_USERNAME=admin.companydomain.com` 此 MSI 属性是未受管桌面的必要属性。 不要将此 MSI 属性用于受 vCenter Server 管理的虚拟机桌面。	无
VDM_SERVER_PASSWORD	View Connection Server 管理员用户密码。 例如：`VDM_SERVER_PASSWORD=secret` 此 MSI 属性是未受管桌面的必要属性。 不要将此 MSI 属性用于受 vCenter Server 管理的虚拟机桌面。	无

在静默安装命令中，您可以使用 MSI 属性 `ADDLOCAL=` 来指定 View Agent 安装程序要配置的自定义功能。每个静默安装功能对应一个在交互安装过程中可以选择的自定义安装选项。

表 4–6 显示了可在命令行中键入的 View Agent 功能以及相应的自定义安装选项。

表 4–6 View Agent 静默安装的功能和交互式自定义安装选项

静默安装功能	交互式安装中的自定义安装选项
Core。 如果您使用 MSI 属性 `ADDLOCAL=` 指定单个功能，则必须将 **Core** 包括在内。 如果您指定 `ADDLOCAL=ALL`，将安装包括 Core 在内的所有功能。	无。 在交互式安装过程中，会默认安装 core View Agent 功能。
SVIAgent	View Composer Agent
ThinPrint	Virtual Printing（虚拟打印）
ThinPrintPCoIP	Virtual Printing with PCoIP（带 PCoIP 的虚拟打印）
PCoIP	PCoIP Protocol（PCoIP 协议）
USB	USB Redirection（USB 重定向）

有关自定义安装选项的详细信息，请参阅第 46 页，“View Agent 自定义安装选项”。

为 View Agent 配置具有多个 NIC 的虚拟机

在具有多个 NIC 的虚拟机上安装 View Agent 时，必须配置 View Agent 使用的子网。子网确定 View Agent 提供给 View Connection Server 实例进行客户端协议连接的网络地址。

步骤

◆ 在安装了 View Agent 的虚拟机上，打开一个命令提示符，并创建一个注册表条目以配置子网。

例如：**`HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = n.n.n.n/m (REG_SZ)`**

在此示例中，*n.n.n.n* 为 TCP/IP 子网，*m* 为子网掩码中的位数。

优化 Windows 客户操作系统性能

您可以执行某些特定步骤来为 View 桌面部署优化客户操作系统性能。这些步骤适用于所有 Windows 操作系统。所有步骤都是可选操作。

前提条件

为 View 桌面部署准备客户操作系统。

步骤

- 禁用任何未使用的端口，如 COM1、COM2 和 LPT。
- 调整显示属性。
  - a 选择一个基本主题。
  - b 将背景设置为某一单色。
  - c 将屏幕保护程序设置为 **[None（无）]**。
  - d 确认已启用硬件加速。
- 选择一个高性能电源选项，并且不指定睡眠计时器。
- 禁用索引服务组件。

  注意 索引功能通过将文件分类来改进搜索性能。对于经常进行搜索的用户，不应禁用此功能。

- 将系统还原点移除或降至最少。
- 关闭 `C:\` 上的系统保护。
- 禁用任何不必要的服务。
- 将声音方案设置为 **[No Sounds（无声）]**。
- 将视觉效果设置为 **[Adjust for best performance（调整为最佳性能）]**。
- 打开 Windows Media Player 并使用默认设置。
- 关闭计算机自动维护。
- 将性能设置调整为最佳性能。
- 删除 `C:\Windows` 中任何隐藏的卸载文件夹，如 `$NtUninstallKB893756$`。
- 删除所有事件日志。
- 运行磁盘清理程序以便移除临时文件、清空回收站并移除系统文件和其他不再需要的内容。
- 运行磁盘碎片整理程序以重新整理碎片数据。

下一步

在 Windows 7 客户操作系统中，可以执行更多优化任务。请参阅第 51 页，“优化 Windows 7 客户操作系统性能”。

优化 Windows 7 客户操作系统性能

您可以执行附加步骤来为 View 桌面部署优化 Windows 7 客户操作系统性能。所有步骤都是可选操作。

前提条件

执行适用于所有 Windows 操作系统的客户操作系统优化步骤。请参阅第 50 页，“优化 Windows 客户操作系统性能”。

步骤

1 卸载 Tablet PC 组件，除非需要此功能。

2 禁用 IPv6，除非需要此功能。

3 启动系统配置实用程序 (`msconfig.exe`) 并配置引导和启动设置。

   a 在 **[Boot（引导）]** 选项卡上，选择 **[No GUI boot（无 GUI 引导）]** 和 **[Base video（基本视频）]**。

   b 在 **[Startup（启动）]** 选项卡上，禁用 Adobe Acrobat 和 Reader。

4 使用文件系统实用程序 (`fsutil`) 命令禁用持续跟踪文件最后访问时间的设置。

   例如：`fsutil behavior set disablelastaccess 1`

5 启动注册表编辑器 (`regedit.exe`) 并将 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Disk** 下的 **TimeOutValue** REG_DWORD 更改为 **`0x000000be(190)`**。

6 关闭客户操作系统和虚拟机。

7 将虚拟机视频卡 RAM 设置更改为 128 MB。

8 启动虚拟机。

下一步

请参阅第 52 页，“为链接克隆桌面优化 Windows 7”，以获取有关如何通过禁用某些 Windows 7 服务和任务来减缓 View Composer 链接克隆桌面增长速度的信息。禁用某些特定服务和任务也可为完整虚拟机带来性能优势。

为链接克隆桌面优化 Windows 7

通过禁用某些 Windows 7 服务和任务，您可以减缓 View Composer 链接克隆桌面的增长速度。禁用某些特定服务和任务也可为完整虚拟机带来性能优势。

禁用 Windows 7 服务和任务所带来的优势

Windows 7 所计划的服务和任务会引发 View Composer 链接克隆增长，即使链接克隆桌面空闲时也是如此。链接克隆操作系统磁盘的不断增长会消耗您在最初创建链接克隆桌面时节省的存储。您可以通过禁用这些 Windows 7 服务减缓链接克隆的增长速度。

Windows 7 会引入新服务并安排默认运行旧服务，如磁盘碎片整理。如果您不禁用这些服务，它们会在后台运行。

影响操作系统磁盘增长的服务在 Windows 7 虚拟机上还会生成每秒输入/输出操作 (input/output operations per second, IPOS)。禁用这些服务可减少 IOPS 并提高整个虚拟机和链接克隆的性能。

禁用特定服务还有利于 Windows XP 和 Windows Vista 操作系统的运行。

这些优化 Windows 7 的最佳实践可应用于大部分用户环境。然而，您必须评估禁用各项服务对您的用户、应用程序和桌面的影响。您可能需要保留特定服务。

例如，如果您刷新和重构链接克隆桌面，就可以禁用 Windows Update 服务。刷新操作会将操作系统磁盘恢复至其上一次快照中的状态，删除自上一次拍摄快照以来所有的 Windows 自动更新。重构操作会从包含当前 Windows 更新的新快照中重新创建操作系统磁盘，这使得 Windows 自动更新成为了一项冗余功能。

如果您不经常使用刷新和重构操作，您可以保留 Windows Update 服务。

对引起链接克隆增长的 Windows 7 服务和任务的概述

某些 Windows 7 服务和任务会导致链接克隆操作系统磁盘每过几小时便逐步增长，即使当链接克隆桌面空闲时也会如此。如果禁用这些服务和任务，您可以控制操作系统磁盘的增长速度。

影响操作系统磁盘增长的服务还会在 Windows 7 虚拟机上产生 IPOS。您可以评估在完整虚拟机以及链接克隆上禁用这些服务的优势。

禁用表 4-7 中显示的 Windows 7 服务之前，请先确定您是否执行了第 50 页，“优化 Windows 客户操作系统性能”和第 51 页，“优化 Windows 7 客户操作系统性能”中的优化步骤。

表 4–7 操作系统空闲时 Windows 7 服务和任务对操作系统磁盘增长和 IOPS 的影响

服务或任务	描述	默认出现或启动时间	对链接克隆操作系统磁盘的影响	对 IOPS 的影响	是否关闭此服务或任务?
Windows 休眠	在电脑关机前将打开的文件和程序存储在一个文件夹中，从而提供一种省电状态。电脑重启时，文件夹将会被重新载入内存，恢复到启动休眠时的状态。	默认电源计划设置会禁用休眠功能。	高。 默认情况下，休眠文件 `hiberfil.sys` 的大小同虚拟机上安装的 RAM 相同。此功能会影响所有客户操作系统。	高。 触发休眠功能后，系统会生成一个与安装的 RAM 同样大小的 `hiberfil.sys` 文件。	是 休眠功能在虚拟环境中没有任何用途。 有关说明，请参阅第 60 页，“在父虚拟机中禁用 Windows 休眠功能”。
Windows 计划的磁盘碎片整理	磁盘碎片整理为计划的后台进程。	一周一次	高。 重复的碎片整理操作会将链接克隆操作系统磁盘增大若干 GB，但也不会提高对链接克隆磁盘的访问效率。	高	是
Windows Update 服务	检测、下载及安装 Windows 和其他程序的更新。	自动启动	中到高。 因为经常执行更新检查，所以会频繁写入链接克隆操作系统磁盘。具体影响取决于所下载的更新。	中到高。	是（如果您使用 View Composer 重构来安装 Windows 更新和执行刷新，并将操作系统磁盘恢复到原始快照中的状态）。
Windows 诊断策略服务	检测、故障排除以及解决 Windows 组件中的问题。如果您停止此服务，诊断功能将不再可用。	自动启动	中到高。 此服务按需触发。根据需要程度，写入频率会有所不同。	低到中	是（如果您不需要诊断工具在桌面运行）。
预取/超级获取	存储您运行的应用程序的特定信息，帮助应用程序更快启动。 此功能在 Windows XP 中引入。	只要不被禁用即始终开启。	中。 导致其布局、数据库信息和单个预取文件（按需生成）的周期性更新。	中。	是（如果您禁用此功能后应用程序启动时所用的时间在可接受的范围内）。
Windows 注册表备份 (`RegIdleBackup`)	系统空闲时自动备份 Windows 注册表。	每 10 天的中午 12:00 点	中。 此任务每次运行时都会生成注册表备份文件。	中。	是。 无需执行 Windows 注册表备份。要还原注册表数据，您可以使用 View Composer 刷新操作。
系统还原	将 Windows 系统恢复至先前的某个正常运行状态。	Windows 启动时进行，之后每天一次。	低到中。 当系统检测到有需要时，捕捉系统还原点。当链接克隆空闲时，此任务的开销很小。	无重大影响。	是 虽然影响较小，但如果您使用 View Composer 刷新功能恢复至操作系统磁盘原始快照中的状态，此任务就属于冗余任务。

表 4–7 操作系统空闲时 Windows 7 服务和任务对操作系统磁盘增长和 IOPS 的影响 （续）

服务或任务	描述	默认出现或启动时间	对链接克隆操作系统磁盘的影响	对 IOPS 的影响	是否关闭此服务或任务?
Windows Defender	提供反间谍软件功能。	Windows 启动时。每天快速扫描一次。每次扫描前均检查更新。	中到高。 执行定义更新、计划扫描以及按需启动的扫描。	中到高。	是（如果安装了其他反间谍软件）。
Microsoft Feeds Synchronization 任务 (`msfeedssync.exe`)	定期更新 Windows Internet Explorer 7 和 8 网络浏览器中的 RSS 源。此任务可更新启用了自动 RSS 源同步功能的 RSS 源。只有当 Internet Explorer 7 或 8 运行时，此进程才会显示在 Windows 任务管理器中。	一天一次。	中。 如果未配置永久磁盘，将会影响操作系统磁盘的增长。如果配置了永久磁盘，将会影响永久磁盘。	中。	是（如果您的用户不要求在其桌面中自动更新 RSS 源）。

禁用 Windows 7 父虚拟机中计划的磁盘碎片整理

创建链接克隆前，您必须禁用 Windows 7 父虚拟机中计划的碎片整理。Windows 7 在默认情况下会计划每周执行一次磁盘碎片整理。重复的碎片整理操作会显著增大链接克隆操作系统磁盘的大小，但不会提高对链接克隆磁盘的访问效率。

当您从父虚拟机上创建链接克隆池时，链接克隆会分享副本的磁盘。后续的碎片整理操作不会影响副本的磁盘，副本磁盘为只读。相反，碎片整理会增加每个克隆的操作系统磁盘的大小。

作为最佳实践，您拍摄快照及创建池之前应对父虚拟机进行一次碎片整理。链接克隆会从碎片整理中获益，因为它们可共享副本的只读优化磁盘。

前提条件

- 确定您想部署在链接克隆上的应用程序已安装在虚拟机上。
- 确认带 View Composer Agent 的 View Agent 已安装在虚拟机上。

步骤

1 在 vSphere Client 中，选择父虚拟机，然后选择 **[Open Console（打开控制台）]**。
2 以管理员身份登录 Windows 7 客户操作系统。
3 单击 **[Start（开始）]** 并在 **[Search programs and files（查找程序和文件）]** 框中键入 `defrag`。
4 在 [Programs（程序）] 窗格中，单击 **[Disk Defragmenter（磁盘碎片整理程序）]**。
5 在 **[Disk Defragmenter（磁盘碎片整理程序）]** 对话框中，单击 **[Defragment disk（整理磁盘碎片）]**。

   磁盘碎片整理程序会在虚拟机硬盘上整合整理过的文件。
6 在 **[Disk Defragmenter（磁盘碎片整理程序）]** 对话框中，单击 **[Configure schedule（配置计划）]**。
7 取消选择 **[Run on a schedule (recommended)（按计划运行（推荐））]**，然后单击 **[OK（确定）]**。

从该父虚拟机创建的链接克隆虚拟机将不会执行碎片整理操作。

禁用 Windows 7 虚拟机中的 Windows Update 服务

禁用 Windows Update 服务可以减少下载和安装更新时创建的文件数量和发生的写入量。此操作可以减缓链接克隆的增长速度，并降低链接克隆和整个虚拟机中的 IPOS。

如果您刷新和重构链接克隆桌面，请禁用 Windows Update 服务。刷新操作会将操作系统磁盘还原至原始快照中捕获的状态，并删除自动进行的 Windows 更新。重构操作会从包含 Windows 更新的新快照中重新创建操作系统磁盘，这使得自动 Windows 更新成为了一项冗余功能。

如果您不使用重构功能在链接克隆中安装 Windows 更新，请勿禁用 Windows Update 服务。

前提条件

确认虚拟机上已下载并安装最新的 Windows 更新。

步骤

1. 在 vSphere Client 中，选择父虚拟机，然后选择 **[Open Console（打开控制台）]**。
2. 以管理员身份登录 Windows 7 客户操作系统。
3. 单击 **[Start（开始）] > [Control Panel（控制面板）] > [System and Security（系统和安全）] > [Turn automatic updating on or off（启用或禁用自动更新）]**。
4. 在 [Important updates（重要更新）] 菜单中，选择 **[Never check for updates（从不检查更新）]**。
5. 取消选择 **[Give me recommended updates the same way I receive important updates（以接收重要更新的相同方式为我提供推荐的更新）]**。
6. 取消选择 **[Allow all users to install updates on this computer（允许所有用户在此计算机上安装更新）]**，然后单击 **[OK（确定）]**。

禁用 Windows 7 虚拟机中的诊断策略服务

禁用 Windows 诊断策略服务能够将系统写入量降至最小，并降低链接克隆桌面的增长速度。

如果您的用户需要在桌面上使用诊断工具，请勿禁用 Windows 诊断策略服务。

步骤

1. 在 vSphere Client 中，选择父虚拟机，然后选择 **[Open Console（打开控制台）]**。
2. 以管理员身份登录 Windows 7 客户操作系统。
3. 单击 **[Start（开始）] > [Control Panel（控制面板）] > [System and Security（系统和安全）] > [Administrative Tools（管理工具）]**。
4. 选择 **[Services（服务）]**，然后单击 **[Open（打开）]**。
5. 双击 **[Diagnostic Policy Service（诊断策略服务）]**。
6. 在 [Diagnostic Policy Service Properties（诊断策略服务属性）]（本地计算机）对话框中，单击 **[Stop（停止）]**。
7. 在 [Startup type（启动类型）] 菜单中，选择 **[Disabled（禁用）]**。
8. 单击 **[OK（确定）]**。

禁用 Windows 7 虚拟机中的预取和超级获取功能

通过禁用 Windows 预取和超级获取功能，您可以避免生成预取文件和与预取及超级获取操作相关的开销。此操作能减缓链接克隆桌面的增长速度，并最大限度减少整个虚拟机和链接克隆中的 IOPS。

要禁用预取和超级获取功能，您必须编辑一个 Windows 注册表项并在虚拟机中禁用预取服务。

前提条件

有关如何在 Windows 7 中使用 Windows 注册表编辑器的信息，请访问 Microsoft TechNet 网站。

步骤

1 在本地 Windows 7 虚拟机上启动 Windows 注册表编辑器。

2 导航至名为 **PrefetchParameters** 的注册表项。

  该注册表项位于以下路径：**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters**。

3 将 **EnablePrefetcher** 和 **EnableSuperfetch** 的值设为 `0`。

4 单击 **[Start（开始）] > [Control Panel（控制面板）] > [System and Security（系统和安全）] > [Administrative Tools（管理工具）]**。

5 选择 **[Services（服务）]**，然后单击 **[Open（打开）]**。

6 双击 **[Superfetch]** 服务。

7 在 [Superfetch Properties (Local Computer)（Superfetch 的属性（本地计算机））] 对话框中，单击 **[Stop（停止）]**。

8 在 [Startup type（启动类型）] 菜单中，选择 **[Disabled（禁用）]**。

9 单击 **[OK（确定）]**。

禁用 Windows 7 虚拟机上的 Windows 注册表备份

禁用Windows 注册表备份功能 (`RegIdleBackup`) 能够将系统写入量降至最小，并降低链接克隆桌面的增长速度。

步骤

1 在 vSphere Client 中，选择父虚拟机，然后选择 **[Open Console（打开控制台）]**。

2 以管理员身份登录 Windows 7 客户操作系统。

3 单击 **[Start（开始）] > [Control Panel（控制面板）] > [System and Security（系统和安全）] > [Administrative Tools（管理工具）]**。

4 选择 **[Task Scheduler（任务计划程序）]**，然后单击 **[Open（打开）]**。

5 在左侧窗格中，展开 **[Task Scheduler Library（任务计划程序库）]**、**[Microsoft]**、**[Windows]**。

6 双击 **[Registry]** 并选择 **[RegIdleBackup]**。

7 在 [Actions（操作）] 窗格中，单击 **[Disable（禁用）]**。

禁用 Windows 7 虚拟机中的系统还原

如果您使用 View Composer 刷新功能将链接克隆操作系统磁盘还原到原始快照中的状态，您无需使用 Windows 系统还原功能。

操作系统空闲时，系统还原对操作系统磁盘增长没有明显影响。然而，操作系统在使用中时，系统还原会根据系统使用情况生成还原点，这会对操作系统磁盘增长产生明显影响。

Windows 系统还原与 View Composer 的刷新功能相同。

作为最佳实践，您可以禁用 Windows 系统还原，从而避免链接克隆不必要的增长。

如果您不适用刷新功能，则需要评估是否在 View 环境保留系统还原功能。

步骤

1 在 vSphere Client 中，选择父虚拟机，然后选择 **[Open Console（打开控制台）]**。

2 以管理员身份登录 Windows 7 客户操作系统。

3 单击 **[Start（开始）]** > **[Control Panel（控制面板）]** > **[System and Security（系统和安全）]** > **[Administrative Tools（管理工具）]**。

4 选择 **[Task Scheduler（任务计划程序）]**，然后单击 **[Open（打开）]**。

5 在左侧窗格中，展开 **[Task Scheduler Library（任务计划程序库）]**、**[Microsoft]**、**[Windows]**。

6 双击 **[SystemRestore]** 并选择 **[SR]**。

7 在 [Actions（操作）] 窗格中，单击 **[Disable（禁用）]**。

禁用 Windows 7 虚拟机上的 Windows Defender

Microsoft Windows Defender 会导致链接克隆操作系统磁盘增长，并增加链接克隆和完整虚拟机中的 IOPS。如果您在虚拟机上安装了其他反间谍软件，请禁用 Windows Defender。

如果虚拟机上只安装了 Windows Defender 一个反间谍软件，您最好在您环境中的桌面上保留 Windows Defender。

步骤

1 在 vSphere Client 中，选择父虚拟机，然后选择 **[Open Console（打开控制台）]**。

2 以管理员身份登录 Windows 7 客户操作系统。

3 单击 **[Start（开始）]** 并在 [Search programs and files（查找程序和文件）] 框中键入 `Windows Defender`。

4 单击 **[Tools（工具）]** > **[Options（选项）]** > **[Administrator（管理员）]**。

5 取消选择 **[Use this program（使用此程序）]** 并单击 **[Save（保存）]**。

禁用 Windows 7 虚拟机中的 Microsoft Feeds Synchronization

Windows Internet Explorer 7 或 8 使用 Microsoft Feeds Synchronization 任务更新用户 Web 浏览器中的 RSS 源。此任务会导致链接克隆的大小增长。如果您的用户浏览器中无需自动 RSS 源更新功能，请禁用此任务。

如果未配置永久磁盘，Microsoft Feeds Synchronization 会导致操作系统磁盘增长。如果配置了永久磁盘，将会影响永久磁盘。在这种情况下，您仍应禁用 Microsoft Feeds Synchronization，以控制永久磁盘的增长。

步骤

1 在 vSphere Client 中，选择父虚拟机，然后选择 **[Open Console（打开控制台）]**。

2 以管理员身份登录 Windows 7 客户操作系统。

3 单击 **[Start（开始）]** > **[Control Panel（控制面板）]** > **[Network and Internet（网络和 Internet）]** > **[Internet Options（Internet 选项）]**。

4 单击 **[Content（内容）]** 选项卡。

5 在 [Feeds and Web Slices（源和网页快讯）] 下，单击 **[Settings（设置）]**。

6 取消选择 **[Automatically check feeds and Web Slices for updates（自动检查源和网页快讯的更新）]** 并单击 **[OK（确定）]**。

7 在 [Internet Properties（Internet 属性）] 对话框中，单击 **[OK（确定）]**。

为 View Composer 准备虚拟机

要部署链接克隆桌面，您必须准备一个符合 View Composer 服务要求的父虚拟机。

- 准备父虚拟机第 58 页，

  View Composer 服务需要通过父虚拟机来生成基础映像，以便创建和管理链接克隆桌面。

- 在链接克隆桌面上激活 Windows 7 和 Windows Vista 第 59 页，

  为确保 View Composer 在链接克隆桌面上正确激活 Windows 7 和 Windows Vista 操作系统，您必须使用父虚拟机上的 Microsoft 卷激活功能。卷激活技术需要使用卷许可证密钥。

- 在父虚拟机中禁用 Windows 休眠功能第 60 页，

  Windows 休眠选项会创建一个巨大的系统文件，这将增加从父虚拟机创建的链接克隆操作系统磁盘的大小。禁用休眠选项能减小链接克隆的大小。

- 将父虚拟机配置为使用本地存储第 61 页，

  为 View Composer 准备父虚拟机时，您可以将父虚拟机和链接克隆桌面配置为在本地数据存储中存储虚拟机交换文件。这种可选策略可帮助您充分利用本地存储。

- 记录父虚拟机的页面文件大小第 61 页，

  创建链接克隆池后，您可以将链接克隆的客户操作系统页面文件和临时文件重定向到一个单独的磁盘。您配置的磁盘大小必须大于客户操作系统页面文件的大小。

- 延长 QuickPrep 自定义脚本的超时限制第 62 页，

  View Composer 会终止运行时间超过 20 秒的 QuickPrep 同步后脚本或关机脚本。通过更改父虚拟机上的 `ExecScriptTimeout` Windows 注册表值，您可以延长超时限制。

准备父虚拟机

View Composer 服务需要通过父虚拟机来生成基础映像，以便创建和管理链接克隆桌面。

前提条件

- 确认您为部署 View 桌面准备了一个虚拟机。请参阅第 41 页，“为 View 桌面部署创建虚拟机”。

  您无需将父虚拟机加入链接克隆桌面将驻留的 Active Directory 域中。父虚拟机可以是本地 WORKGROUP 的一员。

  重要事项 要使用 View Manager 4.5 的功能，如将一次性数据重定向到单独的磁盘以及使用 Sysprep 自定义链接克隆桌面，您必须部署已安装 View Agent 4.5 的父虚拟机上的桌面。

  您不能使用 View Composer 来部署运行 Windows Vista Ultimate Edition 或 Windows XP Professional SP1 的桌面。

- 如果父虚拟机上运行的是 Windows XP，而您的 Active Directory 在 Windows Server 2008 上运行，请在 Windows XP 虚拟机中应用更新修补程序。请参阅 Microsoft 支持文章 944043，该文章位于：http://support.microsoft.com/kb/944043/en-us。http://support.microsoft.com/kb/944043/en-us.

  如果您没有在 Windows XP 上安装 Windows Server 2008 只读域控制器 (RODC) 兼容包，那么从此父虚拟机上部署的链接克隆将无法加入域。

- 在父虚拟机上安装 View Agent 时，应选择 **[View Composer Agent]** 选项。请参阅第 45 页，“在虚拟机中安装 View Agent”。

  要在大型环境中更新 View Agent，您可以使用标准的 Windows 更新机制（如 Altiris、SMS、LanDesk、BMC）或其他系统管理软件。您还可以通过重构操作来更新 View Agent。

- 要部署运行 Windows 7 或 Windows Vista 的桌面，您必须配置卷许可证密钥，并使用卷激活功能激活父虚拟机的操作系统。请参阅第 59 页，“在链接克隆桌面上激活 Windows 7 和 Windows Vista”。
- 如果父虚拟机上运行 Windows 7，请确认您遵循了优化操作系统的最佳实践。请参阅第 52 页，“为链接克隆桌面优化 Windows 7”。

步骤

- 移除父虚拟机上的 DHCP 租期，以避免将租借的 IP 地址复制到池中的链接克隆。

  a 在父虚拟机上打开一个命令提示符。

  b 键入 **`ipconfig /release`** 命令。

- 确认系统磁盘包含一个卷。

  无法通过包含多个卷的父虚拟机来部署链接克隆。View Composer 服务不支持多个磁盘分区，但支持多个虚拟磁盘。

- 禁用休眠选项以减少从父虚拟机创建的链接克隆操作系统磁盘的大小。

您可以通过父虚拟机来部署链接克隆池。如果父虚拟机硬件为版本 7，则创建链接克隆池时应遵循以下规则：

- 将链接克隆池部署在 ESX/ESXi 4.*x* 主机或群集上。链接克隆池不能驻留在 ESX/ESXi 3.5 主机，或者同时包含 ESX/ESXi 4.*x* 主机和 ESX/ESXi 3.5 主机的群集中。
- 在 vSphere 模式下创建链接克隆池。

下一步

使用 vSphere Client 为处于关机状态的父虚拟机拍摄快照。该快照将用作第一组绑定到父虚拟机的链接克隆桌面的基准配置。

重要事项 拍摄快照前，请使用客户操作系统中的 **[Shut Down（关机）]** 命令彻底关闭父虚拟机。

在链接克隆桌面上激活 Windows 7 和 Windows Vista

为确保 View Composer 在链接克隆桌面上正确激活 Windows 7 和 Windows Vista 操作系统，您必须使用父虚拟机上的 Microsoft 卷激活功能。卷激活技术需要使用卷许可证密钥。

要激活 Windows 7 或 Windows Vista 的卷激活功能，您需要使用密钥管理服务 (Key Management Service, KMS)，密钥管理服务需要使用 KMS 许可证密钥。请咨询您的 Microsoft 经销商，获取卷许可证密钥并配置卷激活功能。

注意 View Composer 不支持多激活密钥 (Multiple Activation Key, MAK) 许可。

使用 View Composer 创建链接克隆桌面之前，您必须使用卷激活功能来激活父虚拟机上的操作系统。

注意 具有卷许可证的 Windows XP 桌面不需要激活。

创建链接克隆桌面以及每次重构链接克隆后，View Composer Agent 均会使用父虚拟机的 KMS 服务器来激活链接克隆上的操作系统。

View Composer QuickPrep 工具通过以下步骤执行激活：

1 调用脚本来移除链接克隆虚拟机上现有许可证状态

2 重新启动客户操作系统

3 调用一个使用 KMS 许可的脚本来激活克隆上的操作系统。

每次在链接克隆上运行 QuickPrep 时，都会进行激活。

对于 KMS 许可，View Composer 将使用为激活父虚拟机配置的 KMS 服务器。KMS 服务器将激活的链接克隆视为具有新颁发许可证的计算机。

在父虚拟机中禁用 Windows 休眠功能

Windows 休眠选项会创建一个巨大的系统文件，这将增加从父虚拟机创建的链接克隆操作系统磁盘的大小。禁用休眠选项能减小链接克隆的大小。

Windows 休眠选项会创建一个隐藏的系统文件，即 `Hiberfil.sys`。混合睡眠设置开启时，Windows 会用此文件在硬盘上存储一份系统内存的副本。创建链接克隆池时，每个链接克隆操作系统磁盘中均会创建此文件。

在 Windows 7 虚拟机中，这个文件的大小可达 10 GB。



小心 休眠功能不可用时，混合睡眠设置不能正常工作。开启混合睡眠设置后，如果出现电源中断，用户将丢失数据。

前提条件

熟悉 Windows 休眠功能。请查阅 Microsoft 支持网站。有关在 Windows 7 或 Windows Vista 中禁用休眠功能的信息，请访问 Microsoft 支持网站，在网站中搜索如何在运行 Windows 的计算机上禁用和重新启用休眠功能。

步骤

1 在 vSphere Client 中，选择父虚拟机，然后选择 **[Open Console（打开控制台）]**。

2 以管理员身份登录 Windows 客户操作系统。

3 禁用休眠选项。

操作系统	操作
Windows 7 或 Windows Vista	a 单击 **[Start（开始）]** 并在 **[Start Search（开始搜索）]** 框中键入 **`cmd`**。 b 在搜索结果列表中，右键单击 **[Command Prompt（命令提示符）]** 然后单击 **[Run as Administrator（以管理员帐户运行）]**。 c 在 [User Account Control（用户帐户控制）] 提示中单击 **[Continue（继续）]**。 d 在命令提示符下，键入 **`powercfg.exe /hibernate off`**，然后按 Enter 键。 e 键入 **`exit`**，然后按 Enter 键。
Windows XP	a 单击 **[Start（开始）]** > **[Run（运行）]**。 b 键入 **`cmd`**，然后单击 **[OK（确定）]**。 c 在命令提示符下，键入 **`powercfg.exe /hibernate off`**，然后按 Enter 键。 d 键入 **`exit`**，然后按 Enter 键。

4 退出客户操作系统。

从父虚拟机上创建链接克隆桌面时，链接克隆操作系统磁盘中不会创建 `Hiberfil.sys` 文件。

将父虚拟机配置为使用本地存储

为 View Composer 准备父虚拟机时，您可以将父虚拟机和链接克隆桌面配置为在本地数据存储中存储虚拟机交换文件。这种可选策略可帮助您充分利用本地存储。

在此过程中，您需要配置用于虚拟机交换文件（而不是客户操作系统中的页面文件和临时文件）的本地存储。创建链接克隆池后，您还可以将客户操作系统的页面文件和临时文件重定向到一个单独的磁盘。请参阅第 69 页，“用于创建链接克隆桌面池的工作表”。

前提条件

准备符合 View Composer 服务要求的父虚拟机。请参阅第 58 页，“准备父虚拟机”。

步骤

1 在将要部署链接克隆池的 ESX/ESXi 主机或群集中配置交换文件数据存储。

2 当您在 vCenter Server 中创建父虚拟机时，请将虚拟机交换文件存储在本地 ESX/ESXi 主机或群集中的交换文件数据存储内：

   a 在 vSphere Client 中，选择父虚拟机。

   b 单击 **[Edit Settings（编辑设置）]**，然后单击 **[Options（选项）]** 选项卡。

   c 单击 **[Swapfile location（交换文件位置）]**，然后单击 **[Store in the host's swapfile datastore（存储在主机的交换文件数据存储中）]**。

   有关详细说明，请参阅 VMware vSphere 文档。

当您通过该父虚拟机部署池时，链接克隆桌面将使用本地 ESX 主机的交换文件数据存储。

记录父虚拟机的页面文件大小

创建链接克隆池后，您可以将链接克隆的客户操作系统页面文件和临时文件重定向到一个单独的磁盘。您配置的磁盘大小必须大于客户操作系统页面文件的大小。

如果您为客户操作系统页面文件和临时文件配置一个单独的磁盘，View Manager 将在链接克隆关闭后删除这些一次性文件。此功能可减慢链接克隆的增长速度。但是，只有当您配置的一次性文件磁盘容量足以容纳客户操作系统的页面文件时，才可以使用此功能。

您必须先了解父虚拟机中的最大页面文件大小，才能配置一次性文件磁盘。链接克隆与用来创建它们的父虚拟机具有相同的页面文件大小。

注意 此功能不同于为虚拟机交换文件配置本地存储。请参阅第 61 页，“将父虚拟机配置为使用本地存储”。

步骤

1 在 vSphere Client 中，右键单击父虚拟机，然后单击 **[Open Console（打开控制台）]**。

2 选择 **[Start（开始）] > [Settings（设置）] > [Control Panel（控制面板）] > [System（系统）]**。

3 单击 **[Advanced（高级）]** 选项卡。

4 在 [Performance（性能）] 窗格中，单击 **[Settings（设置）]**。

5 单击 **[Advanced（高级）]** 选项卡。

6 在 [Virtual memory（虚拟内存）] 窗格中，单击 **[Change（更改）]**。

   屏幕上将显示 [Virtual Memory（虚拟内存）] 页面。

7 将页面文件的大小设置为大于分配给虚拟机的内存大小的值。

重要事项 如果 **[Maximum size (MB)（最大大小 (MB)）]** 设置小于虚拟机内存大小，请输入一个大于内存大小的值并保存新值。

8 记录在 [Paging file size for selected drive（所选驱动器的页面文件大小）] 窗格中配置的 **[Maximum size (MB)（最大大小 (MB)）]** 设置。

下一步

通过该父虚拟机配置链接克隆池后，需要配置一个容量大于页面文件的一次性文件磁盘。

延长 QuickPrep 自定义脚本的超时限制

View Composer 会终止运行时间超过 20 秒的 QuickPrep 同步后脚本或关机脚本。通过更改父虚拟机上的 `ExecScriptTimeout` Windows 注册表值，您可以延长超时限制。

延长的超时限制将传播给通过父虚拟机创建的链接克隆。QuickPrep 自定义脚本可以在链接克隆上以您指定的时间长度持续运行。

您也可以使用自定义脚本来启动其他执行长时间运行任务的脚本或进程。

注意 多数 QuickPrep 自定义脚本可以在 20 秒的限制内完成运行。在延长限制之前，请对脚本进行测试。

前提条件

- 使用 **[View Composer Agent]** 选项在父虚拟机上安装 View Agent。
- 确认已准备好父虚拟机来创建链接克隆池。请参阅第 58 页，“准备父虚拟机”。

步骤

1 在父虚拟机上启动 Windows 注册表编辑器。

   a 选择 **[Start（开始）]** > **[Command Prompt（命令提示符）]**。

   b 通过命令提示符键入 **regedit**。

2 在 Windows 注册表中，找到 `vmware-viewcomposer-ga` 注册表项。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl\Set\services\vmware-viewcomposer-ga
```

3 单击 **[Edit（编辑）]**，并修改注册表值。

```
Value Name：ExecScriptTimeout
Value Type：REG_DWORD
Value unit:milliseconds
```

   默认值为 20000 毫秒。

超时值将延长。您不需要重新启动 Windows，该值即可生效。

下一步

拍摄父虚拟机快照并创建链接克隆池。

创建虚拟机模板

您必须先创建虚拟机模板，才能创建自动池。

虚拟机模板是虚拟机的主要副本，可用于创建和部署新的虚拟机。通常情况下，模板中包括已安装的客户操作系统和一组应用程序。

您可以在 vSphere Client 中创建虚拟机模板。您可以通过先前配置的虚拟机创建虚拟机模板，也可以将先前配置的虚拟机转换为虚拟机模板。

有关使用 vSphere Client 创建虚拟机模板的信息，请参阅《*vSphere Basic System Administration*》（vSphere 基础系统管理）指南。有关创建自动池的信息，请参阅第 65 页，“包含完整虚拟机的自动池”。

注意 您不能从虚拟机模板创建链接克隆池。

创建自定义规范

自定义规范不是必需的，但是通过提供许可、域附属和 DHCP 设置等常规属性的配置信息，自定义规范可以大幅提高自动池部署速度。

利用自定义规范，您可以在从 View Administrator 时创建 View 桌面时对桌面进行自定义。您需要在 vSphere Client 中使用 [Customization Specification（自定义规范）] 向导创建新的自定义规范。此外，使用 [Customization Specification（自定义规范）] 向导还可以导入现有自定义 `sysprep.ini` 文件。

有关使用 [Customization Specification（自定义规范）] 向导的信息，请参阅《*vSphere Basic System Administration*》（vSphere 基础系统管理）指南。

注意 要将自定义规范应用于使用 Windows XP 的桌面池，您必须在 vCenter Server 计算机中安装 Microsoft Sysprep 工具。

对于使用 Windows 7 或 Vista 的桌面池，则不需要在 vCenter Server 中安装 Sysprep 工具。这些操作系统中内置了 Sysprep 工具。

当您使用 Sysprep 自定义规范将 Windows 7 桌面加入一个域中时，您必须使用 Active Directory 域的主机域名全称 (Fully Qualified Domain Name, FQDN)。不能使用 Active Directory 域的 NetBIOS 名称。

创建桌面池 5

您可以使用 View Manager 创建桌面池，从而向客户端交付 View 桌面访问。View Manager 将从桌面源部署池，桌面源可以是 vCenter Server 管理的虚拟机、在其他虚拟化平台上运行的虚拟机，也可以是物理机、终端服务器或刀片 PC。

您可以创建多种类型的桌面池，也可以使用单个桌面源来部署手动池，从而部署单个桌面。

- 包含完整虚拟机的自动池第 65 页，

  为创建自动桌面池，View Manager 会根据您应用于该池的设置动态部署桌面。View Manager 使用一个虚拟机模板作为池的桌面源，在 vCenter Server 中为每个桌面创建一个新虚拟机。

- 链接克隆桌面池第 69 页，

  为创建链接克隆桌面池，View Composer 会从一个父虚拟机的某个快照生成链接克隆虚拟机。View Manager 将根据您应用于该池的设置动态部署链接克隆桌面。

- 手动桌面池第 85 页，

  为创建手动桌面池，View Manager 会从现有的桌面源部署桌面。对于池中每个桌面，您需要选择一个单独的桌面源来向客户端交付 View 访问。

- Microsoft 终端服务池第 89 页，

  您可以使用 Microsoft 终端服务器将终端服务会话作为桌面提供给 View 客户端。View Manager 管理终端服务会话的方式与管理其他 View 桌面的方式相同。

- 部署桌面池第 90 页，

  创建桌面池时，您需要选择配置选项，从而确定池的管理方式，以及用户与桌面的交互方式。

- 为桌面池设置电源策略第 98 页，

  您可以为桌面池中由 vCenter Server 管理的虚拟机配置电源策略。

包含完整虚拟机的自动池

为创建自动桌面池，View Manager 会根据您应用于该池的设置动态部署桌面。View Manager 使用一个虚拟机模板作为池的桌面源，在 vCenter Server 中为每个桌面创建一个新虚拟机。

用于创建包含完整虚拟机的自动池的工作表

当您创建自动桌面池时，View Administrator 的 [Add Pool（添加池）] 向导会提示您配置特定选项。您可以使用此工作表在创建池之前准备配置选项。

您可以打印此工作表，并记下您要在运行 [Add Pool（添加池）] 向导时指定的值。

要创建链接克隆池，请参阅第 69 页，“链接克隆桌面池”。

表 5–1 工作表：用于创建包含完整虚拟机的自动池的配置选项

选项	描述	在此填写您要指定的值
User assignment（用户分配）	选择用户分配类型： ■ 在专用分配池中，每个用户会分配给一个桌面。用户每次登录时会收到相同的桌面。 ■ 在浮动分配池中，用户每次登录时都会接收到不同的桌面。 有关详细信息，请参阅第 91 页，“桌面池中的用户分配”。	
Enable automatic assignment（启用自动分配）	在专用分配池中，将在用户首次登录池时为该用户分配一个桌面。您还可以将桌面明确分配给用户。 如果不启用自动分配，则必须为每个用户明确分配桌面。	
vCenter Server	选择用于管理池中虚拟机的 vCenter Server。	
Pool ID（池 ID）	用于在 View Administrator 中标识池的唯一名称。 如果您的环境中运行了多个 vCenter Server，应确保其他 vCenter Server 没有使用同一个池 ID。 View Connection Server 配置可以是一个独立的 View Connection Server 实例，也可以是一个共享通用 View LDAP 配置的副本实例组。	
Display name（显示名称）	用户通过 View Client 登录时看到的池名称。如果不指定显示名称，系统将向用户显示池 ID。	
View Folder（View 文件夹）	选择用来存放池的 View 文件夹，或者将池保留在默认的根文件夹下。 如果使用 View 文件夹，则可以将池的管理委托给某个具有特定角色的管理员。有关详细信息，请参阅第 22 页，“使用文件夹委托管理”。 **注意** View 文件夹不同于用来存储桌面虚拟机的 vCenter Server 文件夹。稍后，您需要在向导中选择存储其他 vCenter Server 设置的 vCenter Server 文件夹。	
Delete desktop after logoff（注销后删除桌面）	如果您选择浮动用户分配，需要选择是否在用户注销后删除桌面。 **注意** 在 [Pool Settings（池设置）] 页面中设置此选项。	
Pool Settings（池设置）	这些设置用于确定桌面状态、虚拟机处于未使用状态时的电源状态、显示协议、Adobe Flash 质量等。 有关说明，请参阅第 96 页，“桌面和池的设置”。 有关适用于自动池的设置列表，请参阅第 68 页，“包含完整虚拟机的自动池的桌面设置”。 有关电源策略和自动池的更多信息，请参阅第 98 页，“为桌面池设置电源策略”。	
Virtual machine naming（虚拟机命名）	选择通过手动指定桌面名称列表，还是通过提供命名模式和桌面总数来部署桌面。 有关详细信息，请参阅第 91 页，“手动命名桌面或提供命名模式”。	
List of desktop names（桌面名称列表）	如果要手动指定名称，需要准备一个文本文件来列出桌面名称，也可以选择性地列出关联的用户名称。	
Naming pattern（命名模式）	如果要采用这种命名方式，则需要提供命名模式。 View Manager 将使用您提供的模式作为所有桌面名称的前缀，并后加一个唯一的编号来标识各个桌面。 有关详细信息，请参阅第 93 页，“为自动桌面池使用命名模式”。	

表 5–1 工作表：用于创建包含完整虚拟机的自动池的配置选项 （续）

选项	描述	在此填写您要指定的值
Maximum Number of desktops（最大桌面数）	如果您使用命名模式，需要指定池中的桌面总数。 您还可以指定在首次创建池时要部署的最小桌面数。	
Number of spare (powered-on) desktops（备用的开机桌面数量）	如果手动指定名称或者使用某种命名模式，需要指定 View Manager 为新用户保留的可用且开机的桌面数量。有关详细信息，请参阅第 91 页，“手动命名桌面或提供命名模式”。 当您手动指定名称时，此选项名为 **[# Unassigned desktops kept powered on（保持开机状态的未分配桌面数）]**。	
Minimum Number of desktops（最小桌面数）	如果您使用命名模式，并根据需要部署桌面，则需要指定池中的最小桌面总数。 如果根据需要部署桌面，View Manager 将在用户首次连接到池时创建桌面。 View Manager 会在您创建池时创建最小数量的桌面。	
Template（模板）	选择 View Manager 用于创建池的虚拟机模板。	
vCenter Server folder（vCenter Server 文件夹）	选择要在其中驻留桌面池的 vCenter Server 文件夹。	
Host or cluster（主机或群集）	选择要在其中运行桌面虚拟机的 ESX 主机或群集。	
Resource pool（资源池）	选择要在其中驻留桌面池的 vCenter Server 资源池。	
Datastores（数据存储）	选择一个或多个要在其中存储桌面池的数据存储区。 对于群集，您可以使用共享或本地数据存储。	
Guest customization（客户机自定义）	从列表中选择一种自定义规范 (SYSPREP)，以供 View Manager 配置许可、域附属、DHCP 设置以及桌面上的其他属性。 或者，您也可以在 View Manager 创建桌面后手动自定义桌面。	

创建包含完整虚拟机的自动池

您可以根据所选择的虚拟机模板来创建自动桌面池。View Manager 可动态部署桌面，并在 vCenter Server 中为每个桌面创建新虚拟机。

要创建链接克隆池，请参阅第 69 页，“链接克隆桌面池”。

前提条件

- 准备一个 View Manager 创建桌面时所需使用的虚拟机模板。该模板上必须安装了 View Agent。请参阅第 41 页，第 4 章“创建和准备虚拟机”。
- 收集您在创建池时必须提供的配置信息。请参阅第 65 页，“用于创建包含完整虚拟机的自动池的工作表”。
- 确定如何配置电源设置、显示协议、Adobe Flash 质量及其他设置。请参阅第 96 页，“桌面和池的设置”。

步骤

1. 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。
2. 单击 **[Add（添加）]**。
3. 选择 **[Automated Pool（自动池）]**。

4 从 [vCenter Server] 页面上选择 **[Full virtual machines（完整虚拟机）]**。

5 按照向导中的提示创建池。

使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称，您可以直接返回至已完成的任意向导页面。

要查看添加到池的桌面，您可以在 View Administrator 中单击 **[Inventory（清单）]** > **[Desktops（桌面）]**。

下一步

授予用户访问池的权限。请参阅第 103 页，“向桌面池添加授权”。

包含完整虚拟机的自动池的桌面设置

配置包含完整虚拟机的自动池时，您必须指定桌面和池的设置。适用于专用用户分配池和浮动用户分配池的设置有所不同。

表 5-2 列出了适用于专用分配自动池和浮动分配自动池的设置。

有关每种桌面设置的描述，请参阅第 96 页，“桌面和池的设置”。

表 5–2 包含完整虚拟机的自动池设置

设置	专用分配自动池	浮动分配自动池
State（状态）	是	是
Connection Server restrictions（Connection Server 限制）	是	是
Remote desktop power policy（远程桌面电源策略）	是	是
Automatic logoff after disconnect（断开连接后自动注销）	是	是
Allow users to reset their desktops（允许用户重置桌面）	是	是
Allow multiple sessions per user（允许每个用户多个会话）		是
Delete desktop after logoff（注销后删除桌面）		是
Default display protocol（默认显示协议）	是	是
Allow users to choose protocol（允许用户选择协议）	是	是
Max number of monitors（显示器最大数量）	是	是
Max resolution of any one monitor（任意一台显示器的最大分辨率）	是	是
Adobe Flash quality（Adobe Flash 质量）	是	是
Adobe Flash throttling（Adobe Flash 调节）	是	是

链接克隆桌面池

为创建链接克隆桌面池，View Composer 会从一个父虚拟机的某个快照生成链接克隆虚拟机。View Manager 将根据您应用于该池的设置动态部署链接克隆桌面。

由于链接克隆桌面会共享一个基础系统磁盘映像，因此它们使用的存储空间比完整虚拟机要少。

用于创建链接克隆桌面池的工作表

当您创建链接克隆桌面池时，View Administrator 的 [Add Pool（添加池）] 向导会提示您配置特定选项。您可以使用此工作表在创建池之前准备配置选项。

您可以打印此工作表，并记下您要在运行 [Add Pool（添加池）] 向导时指定的值。

在创建链接克隆池之前，您必须使用 vCenter Server 为准备用作池的父虚拟机拍摄快照。为父虚拟机拍摄快照之前必须将其关闭。View Composer 将使用该快照作为基础映像来创建克隆。

注意 您不能从虚拟机模板来创建链接克隆池。

表 5–3 工作表：用于创建链接克隆桌面池的配置选项

选项	描述	在此填写您要指定的值
User assignment（用户分配）	选择用户分配类型： ■ 在专用分配池中，每个用户会分配给一个桌面。用户每次登录时会收到相同的桌面。 ■ 在浮动分配池中，用户每次登录时都会接收到不同的桌面。 有关详细信息，请参阅第 91 页，“桌面池中的用户分配”。	
Enable automatic assignment（启用自动分配）	在专用分配池中，将在用户首次登录池时为该用户分配一个桌面。您还可以将桌面明确分配给用户。 如果不启用自动分配，则必须为每个用户明确分配桌面。	
vCenter Server	选择用于管理池中虚拟机的 vCenter Server。	
Pool ID（池 ID）	用于在 View Administrator 中标识池的唯一名称。 如果您的环境中运行了多个 View Connection Server 配置，应确保其他 View Connection Server 配置未使用同一个池 ID。 View Connection Server 配置可以是一个独立的 View Connection Server 实例，也可以是一个共享通用 View LDAP 配置的副本实例组。	
Display name（显示名称）	用户通过 View Client 登录时看到的池名称。如果不指定显示名称，系统将向用户显示池 ID。	
View Folder（View 文件夹）	选择用来存放池的 View 文件夹，或者将池保留在默认的根文件夹下。 如果使用 View 文件夹，则可以将池的管理委托给某个具有特定角色的管理员。有关详细信息，请参阅第 22 页，“使用文件夹委托管理”。 **注意** View 文件夹不同于用来存储桌面虚拟机的 vCenter Server 文件夹。稍后，您需要在向导中选择存储其他 vCenter Server 设置的 vCenter Server 文件夹。	
Delete or refresh desktop on logoff（注销时删除或刷新桌面）	如果您选择浮动用户分配，需要选择在用户注销后刷新桌面、删除桌面，还是不执行任何操作。 **注意** 在 [Pool Settings（池设置）] 页面中设置此选项。	

表 5–3 工作表：用于创建链接克隆桌面池的配置选项（续）

选项	描述	在此填写您要指定的值
Pool Settings（池设置）	这些设置用于确定桌面状态、虚拟机处于未使用状态时的电源状态、显示协议、Adobe Flash 质量等。 有关说明，请参阅第 96 页，“桌面和池的设置”。 有关适用于链接克隆池的设置列表，请参阅第 74 页，“链接克隆桌面池的桌面设置”。 有关电源策略和自动池的更多信息，请参阅第 98 页，“为桌面池设置电源策略”。	
Redirect Windows profile to persistent disks（将 Windows 配置文件重定向到永久磁盘）	如果您选择专用用户分配，需要选择将 Windows 用户配置文件数据存储在一个单独的 View Composer 永久磁盘上，还是与操作系统数据存储在同一磁盘上。 您可以使用单独的永久磁盘保留用户数据和设置。View Composer 刷新、重构和重新平衡操作不会影响永久磁盘。您可以将永久磁盘从一个链接克隆中分离，并连接到另一个桌面。 如果将 Windows 配置文件存储在操作系统磁盘中，则在刷新、重构和重新平衡操作过程中，用户数据和设置将被移除。	
Disk size and drive letter for persistent disk（永久磁盘的磁盘大小和驱动器盘符）	如果将用户配置文件数据存储在一个单独的 View Composer 永久磁盘中，则需要提供磁盘大小（以 MB 为单位）和驱动器盘符。 **注意** 不要选择父虚拟机上已经存在的驱动器盘符，或者与网络上装载的驱动器所用的驱动器盘符冲突的驱动器盘符。	
Disposable File Redirection（一次性文件重定向）	选择是否将客户操作系统的页面文件和临时文件重定向到一个单独的非永久磁盘。如果选择这样做，则需要指定磁盘大小（以 MB 为单位）。 如果进行此配置，View Manager 会在链接克隆关闭后删除一次性文件。链接克隆的大小在用户与其桌面交互过程中会增长。一次性文件重定向可以减缓链接克隆的增长速度，从而节省存储空间。 磁盘大小应大于客户操作系统的页面文件大小。要确定页面文件的大小，请参阅第 61 页，“记录父虚拟机的页面文件大小”。 配置一次性文件磁盘大小时，需注意格式化磁盘分区的实际大小比您在 View Administrator 中提供的值略小。 一次性文件重定向仅在 vSphere 模式中受支持。	
Virtual machine naming（虚拟机命名）	选择通过手动指定桌面名称列表，还是通过提供命名模式和桌面总数来部署桌面。 有关详细信息，请参阅第 91 页，“手动命名桌面或提供命名模式”。	
List of desktop names（桌面名称列表）	如果要手动指定名称，需要准备一个文本文件来列出桌面名称，也可以选择性地列出关联的用户名称。	
Naming pattern（命名模式）	如果要采用这种命名方式，则需要提供命名模式。 View Manager 将使用您提供的模式作为所有桌面名称的前缀，并后加一个唯一的编号来标识各个桌面。 有关详细信息，请参阅第 93 页，“为自动桌面池使用命名模式”。	
Maximum Number of desktops（最大桌面数）	如果您使用命名模式，需要指定池中的桌面总数。 您还可以指定在首次创建池时要部署的最小桌面数。	

表 5–3 工作表：用于创建链接克隆桌面池的配置选项 （续）

选项	描述	在此填写您要指定的值
Number of spare (powered-on) desktops（备用的开机桌面数量）	如果手动指定名称或者使用某种命名模式，需要指定 View Manager 为新用户保留的可用且开机的桌面数量。有关详细信息，请参阅第 91 页，“手动命名桌面或提供命名模式”。 当您手动指定名称时，此选项名为 **[# Unassigned desktops kept powered on（保持开机状态的未分配桌面数）]**。	
Minimum Number of desktops（最小桌面数）	如果您使用命名模式，并根据需要部署桌面，则需要指定池中的最小桌面总数。 如果根据需要部署桌面，View Manager 将在用户首次连接到池时创建桌面。 View Manager 会在您创建池时创建最小数量的桌面。	
Parent virtual machine（父虚拟机）	为池选择父虚拟机。 要使用 View Manager 4.5 的功能，如将一次性数据重定向到单独的磁盘以及使用 Sysprep 自定义链接克隆，您必须选择一个已安装 View Agent 4.5 的父虚拟机。 **注意** 您不能使用 View Composer 来部署运行 Windows Vista Ultimate Edition 或 Windows XP Professional SP1 的桌面。	
Default image (snapshot)（默认映像（快照））	选择要用作池的基础映像的父虚拟机快照。	
Publish base image to the Transfer Server repository（将基础映像发布到 Transfer Server 存储库中）	如果您使用池来部署本地桌面，请选择此选项。部署本地桌面后，View Transfer Server 会将基础映像从 Transfer Server 存储库下载到客户端。 您也可以在创建池后发布基础映像。	
vCenter Server folder（vCenter Server 文件夹）	选择要在其中驻留桌面池的 vCenter Server 文件夹。	
Host or cluster（主机或群集）	选择要在其中运行桌面虚拟机的 ESX 主机或群集。 如果您不设置 vSphere 模式，可以在包含 ESX/ESXi 4 主机与 ESX/ESXi 3 主机的群集上部署链接克隆池。	
Use vSphere mode for View Composer（为 View Composer 应用 vSphere 模式）	如果您选择仅包含 ESX 4 主机的群集，则可以在 vSphere 模式下创建池。 **重要事项** 某些 View Composer 功能仅在 vSphere 模式下可用。 有关详细信息，请参阅第 75 页，“为 View Composer 应用 vSphere 模式”。	
Resource pool（资源池）	选择要在其中驻留桌面池的 vCenter Server 资源池。	

表 5–3 工作表：用于创建链接克隆桌面池的配置选项 （续）

选项	描述	在此填写您要指定的值
Select Datastores（选择数据存储）	选择一个或多个要在其中存储桌面池的数据存储区。 [Add Pool（添加池）] 向导 **[Select Datastores（选择数据存储）]** 页面中的表格为预估池的存储需求提供了高级指导信息。这些信息能帮助您确定哪个数据存储有足够空间存储链接克隆磁盘。有关详细信息，请参阅第 79 页，"链接克隆桌面池的存储大小"。 ■ 如果您将用户数据和操作系统数据存储在不同的磁盘上，则可以将永久磁盘和操作系统磁盘存储在不同的数据存储中。 ■ 您可以将副本（主）虚拟机存储在高性能数据存储中，将链接克隆存储在单独的数据存储中。 此功能只可在 vSphere 模式中使用。 有关详细信息，请参阅第 83 页，"将 View Composer 副本和链接克隆存储在单独的数据存储中"。 对于群集，您可以使用共享数据存储。在 vSphere 模式下，可以使用共享或本地数据存储。 有关为链接克隆创建的磁盘的更多信息，请参阅第 84 页，"链接克隆桌面的数据磁盘"。	
Storage Overcommit（存储过载）	确定 View Manager 在每个数据存储中创建链接克隆桌面时依据的存储过载级别。 随着级别的增加，数据存储上装载的链接克隆会越来越多，而为单个克隆的增长所保留的空间则越来越少。如果设置较高的存储过载级别，您创建的链接克隆的总逻辑大小就可以大于数据存储的物理存储限制。有关详细信息，请参阅第 82 页，"设置链接克隆桌面的存储过载级别"。	
Active Directory domain（Active Directory 域）	选择 Active Directory 域和用户名。 View Composer 要求使用特定用户特权来创建链接克隆池。QuickPrep 或 Sysprep 会使用域和用户帐户来自定义链接克隆桌面。有关详细信息，请参阅第 13 页，"为 View Composer 创建用户帐户"。 当您为 vCenter Server 配置 View Composer 设置时，应指定此用户。有关详细信息，请参阅第 14 页，"为 vCenter Server 配置 View Composer 设置"。当您配置 View Composer 设置时，可以指定多个域和用户。当您使用 [Add Pool（添加池）] 向导创建池时，必须从列表中选择一个域和用户。	
Active Directory container（Active Directory 容器）	提供 Active Directory 容器的相对可区分名称。 例如：`CN=Computers` 当您运行 [Add Pool（添加池）] 向导时，可以浏览 Active Directory 树以找到所需的容器。	
Use QuickPrep or a customization specification (Sysprep)（使用 QuickPrep 或自定义规范 (Sysprep)）	选择使用 QuickPrep 还是某种自定义规范 (SYSPREP)，以供 View Manager 配置许可、域附属、DHCP 设置以及桌面上的其他属性。 Sysprep 只在 vSphere 模式和 vSphere 4.1 软件中受支持。在 vSphere 4.0 或 VMware Infrastructure 3.5 软件中无法使用 Sysprep 自定义链接克隆桌面。 如果您在创建池时使用了 QuickPrep 或 Sysprep，在该池中创建或重构桌面时，无法改为使用其他自定义方法。 有关详细信息，请参阅第 77 页，"选择 QuickPrep 或 Sysprep 来自定义链接克隆桌面"。	

表 5–3 工作表：用于创建链接克隆桌面池的配置选项 （续）

选项	描述	在此填写您要指定的值
Power-off script（关机脚本）	QuickPrep 可以在链接克隆桌面关闭之前在桌面上运行自定义脚本。 需要在父虚拟机中提供指向脚本的路径。	
Post synchronization script（同步后脚本）	QuickPrep 可以在链接克隆桌面创建、重构和刷新之后在桌面上运行自定义脚本。 需要在父虚拟机中提供指向脚本的路径。	

创建链接克隆桌面池

您可以根据所选择的父虚拟机来创建自动链接克隆桌面池。View Composer 服务可在 vCenter Server 中为每个桌面动态创建新的链接克隆虚拟机。

要创建包含完整虚拟机的自动池，请参阅第 65 页， “包含完整虚拟机的自动池”。

前提条件

- 确认 vCenter Server 中安装了 View Composer 服务，并已配置 View Composer 数据库。请参阅《*VMware View 安装指南*》。
- 确认在 View Administrator 中配置了适用于 vCenter Server 的 View Composer 设置。请参阅第 14 页，“为 vCenter Server 配置 View Composer 设置”。
- 确认已准备好父虚拟机。该父虚拟机上必须安装 View Agent。请参阅第 41 页，第 4 章“创建和准备虚拟机”。
- 在 vCenter Server 中为父虚拟机拍摄一个快照。为父虚拟机拍摄快照之前必须将其关闭。View Composer 将使用该快照作为基础映像来创建克隆。

  注意 您不能从虚拟机模板来创建链接克隆池。

- 收集您在创建池时必须提供的配置信息。请参阅第 69 页， “用于创建链接克隆桌面池的工作表”。
- 确定如何配置电源设置、显示协议、Adobe Flash 质量及其他设置。请参阅第 96 页， “桌面和池的设置”。

重要事项 创建链接克隆池时，不要在 vCenter Server 中修改父虚拟机。例如，不要将父虚拟机转换为模板。View Composer 服务要求父虚拟机在池创建过程中保持静止不变的状态。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 单击 **[Add（添加）]**。

3 选择 **[Automated Pool（自动池）]**。

4 从 [vCenter Server] 页面上选择 **[View Composer linked clones（View Composer 链接克隆）]**。

5 按照向导中的提示创建池。

   使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称，您可以直接返回至已完成的任意向导页面。

   在 **[vCenter Settings（vCenter 设置）]** 页面，您必须单击 **[Browse（浏览）]** 并按顺序选择 vCenter Server 设置。您不能跳过任何 vCenter Server 设置：

   a Default image（默认映像）

   b Virtual machine folder（虚拟机文件夹）

   c Host or cluster（主机或群集）

   d Resource pool（资源池）

   e Datastores（数据存储）

要查看添加到池的桌面，您可以在 View Administrator 中单击 **[Inventory（清单）]** > **[Desktops（桌面）]**。

链接克隆在部署期间可能会重新启动一次或多次。

View Composer 还会创建一个用作主映像的副本虚拟机，以供部署链接克隆。为减少占用的空间，该副本将被创建为一个精简磁盘。如果重构或删除了所有桌面，且没有任何克隆链接到副本，则系统将把副本虚拟机从 vCenter Server 中删除。

如果您未将副本存储在单独的数据存储中，View Composer 会在创建链接克隆的每个数据存储中创建一个副本。

如果您将副本存储在单独的数据存储中，则 View Composer 将为整个池创建一个副本，即使链接克隆是在多个数据存储上创建的。

下一步

授予用户访问池的权限。请参阅第 103 页，“向桌面池添加授权”。

链接克隆桌面池的桌面设置

配置包含由 View Composer 创建的链接克隆桌面的自动池时，您必须指定桌面和池的设置。适用于专用用户分配池和浮动用户分配池的设置有所不同。

表 5-4 列出了适用于专用分配和浮动分配链接克隆池的设置。

有关每种桌面设置的描述，请参阅第 96 页，“桌面和池的设置”。

表 5–4 链接克隆桌面自动池的设置

设置	专用分配链接克隆池	浮动分配链接克隆池
State（状态）	是	是
Connection Server restrictions（Connection Server 限制）	是	是
Remote desktop power policy（远程桌面电源策略）	是	是
Automatic logoff after disconnect（断开连接后自动注销）	是	是
Allow users to reset their desktops（允许用户重置桌面）	是	是
Allow multiple sessions per user（允许每个用户多个会话）		是
Delete or refresh desktop on logoff（注销时删除或刷新桌面）		是

表 5–4 链接克隆桌面自动池的设置 （续）

设置	专用分配链接克隆池	浮动分配链接克隆池
Refresh OS disk after logoff（注销后刷新操作系统磁盘）	是	
Default display protocol（默认显示协议）	是	是
Allow users to choose protocol（允许用户选择协议）	是	是
Max number of monitors（显示器最大数量）	是	是
Max resolution of any one monitor（任意一台显示器的最大分辨率）	是	是
Adobe Flash quality（Adobe Flash 质量）	是	是
Adobe Flash throttling（Adobe Flash 调节）	是	是

为 View Composer 应用 vSphere 模式

在 vSphere 模式下，View Composer 部署链接克隆桌面的速度比早期版本快得多。某些 View Composer 功能仅在 vSphere 模式下可用。

您必须在运行 ESX/ESXi 4 或更高版本的主机上创建链接克隆虚拟机，并且必须在 vSphere 模式下配置链接克隆池，才能利用下面这些 View Composer 和 vSphere 功能：

- 将链接克隆虚拟机存储在本地数据存储中
- 将一次性数据重定向到单独的非永久磁盘
- 将副本和链接克隆存储在不同的数据存储中
- 从一个所使硬件版本为 7 的父虚拟机快照创建池
- 为链接克隆虚拟机使用 Sysprep 自定义规范

  此外，Sysprep 仅在 vSphere 4.1 软件中创建的链接克隆上受支持。您无法在 vSphere 4.0 或 VMware Infrastructure 3.5 软件中使用 Sysprep。

vSphere 模式采用了一种在 ESX/ESXi 4 或更高版本上运行的新 API。这种 API 可减少 View Composer 所需的 API 调用数量，因此能加快部署速度。ESX/ESXi 4 可以利用主机上的新硬件功能。

在 vSphere 模式下创建或编辑链接克隆池后，无法将其还原至旧的 API。

在您创建链接克隆池时，ESX/ESXi 的版本决定了 vSphere 模式是否可用：

- 如果您选择仅包含 ESX/ESXi 4 主机的群集，则可以启用 vSphere 模式。如果您计划在群集中部署 ESX/ESXi 3.5 主机，则不能启用 vSphere 模式。如果群集中包含 ESX/ESXi 3.5 主机，您将不能部署、刷新或重构在 vSphere 模式下创建的链接克隆池。

  通过在创建链接克隆池时选中 **[Use vSphere mode for View Composer（为 View Composer 应用 vSphere 模式）]** 复选框，您可以启用此功能。
- 如果您选择单个 ESX/ESXi 4 主机，则必须使用 vSphere 模式。您不能取消选中 **[Use vSphere mode for View Composer（为 View Composer 应用 vSphere 模式）]** 复选框。
- 如果您选择 ESX/ESXi 3.5 主机或包含 ESX/ESXi 3.5 主机的群集，则不能使用 vSphere 模式。

View Composer 对链接克隆 SID 和第三方应用程序的支持

在某些情形下，View Composer 可以为链接克隆虚拟机生成并保留本地计算机安全标识符 (SID)。View Composer 可保留第三方应用程序的全局唯一标识符 (GUID)，具体情况根据应用程序生成 GUID 的方式而定。

要了解 View Composer 操作如何对 SID 和应用程序 GUID 产生影响，您应了解链接克隆桌面的创建和部署方式：

1 View Composer 通过以下操作创建链接克隆：

   a 通过克隆父虚拟机快照创建副本。

   b 创建可以将副本作为其父磁盘引用的链接克隆。

2 View Composer 和 View Manager 使用 QuickPrep 或 Sysprep 自定义规范对链接克隆进行自定义（具体取决于您在创建池时选择的自定义工具）。

   - 如果您使用 Sysprep，系统将为每个克隆生成一个唯一 SID。
   - 如果您使用 QuickPrep，将不生成新的 SID。父虚拟机的 SID 将被复制到池中部署的所有链接克隆桌面上。
   - 某些应用程序会在自定义期间生成 GUID。

3 View Manager 将创建链接克隆的快照。

   该快照包含由 Sysprep 生成的唯一 SID，或者由 QuickPrep 生成的通用 SID。

4 View Manager 按照您在创建池时选择的设置启动桌面。

   某些应用程序会在桌面首次启动时生成 GUID。

有关 QuickPrep 与 Sysprep 自定义的比较，请参阅第 77 页，“选择 QuickPrep 或 Sysprep 来自定义链接克隆桌面”。

当您刷新链接克隆时，View Composer 会使用快照将克隆还原到其初始状态。其 SID 会被保留。

如果您使用的是 QuickPrep，当重构链接克隆时，父虚拟机的 SID 将保留在链接克隆上（只要您为重构操作选择同一父虚拟机）。如果为重构操作选择不同的父虚拟机，新父虚拟机的 SID 将被复制到克隆上。

如果您使用的是 Sysprep，将始终在克隆上生成新的 SID。有关详细信息，请参阅第 79 页，“重构使用 Sysprep 自定义的链接克隆”。

表 5‑5 显示了 View Composer 操作对链接克隆 SID 和第三方应用程序 GUID 的影响。

表 5‑5 View Composer 操作、链接克隆 SID，以及应用程序 GUID

对 SID 或 GUID 的支持	克隆创建	刷新	重构
Sysprep：为链接克隆生成唯一 SID	使用 Sysprep 自定义时，会为链接克隆生成唯一 SID。	保留唯一 SID。	不保留唯一 SID。
QuickPrep：为链接克隆生成通用 SID	利用 QuickPrep 自定义，可为池中的所有克隆生成一个通用 SID。	保留通用 SID。	保留通用 SID。
第三方应用程序 GUID	每个应用程序都具有不同的行为。 **注意** Sysprep 和 QuickPrep 对 GUID 保留产生的影响相同。	如果应用程序在拍摄初始快照之前生成 GUID，将会保留 GUID。 如果应用程序在拍摄初始快照之后生成 GUID，则不会保留 GUID。	重构操作不会保留应用程序 GUID，除非应用程序将 GUID 写入被指定为 View Composer 永久磁盘的驱动器上。

选择 QuickPrep 或 Sysprep 来自定义链接克隆桌面

QuickPrep 和 Microsoft Sysprep 为自定义链接克隆桌面提供了不同的方式。QuickPrep 专为与 View Composer 协同高效工作而设计。Microsoft Sysprep 可提供标准的自定义工具。

创建链接克隆桌面时，您必须修改每个虚拟机，使其能够作为网络中唯一的计算机使用。View Manager 和 View Composer 提供了两种个性化链接克隆桌面的方式。

表 5-6 将 QuickPrep 和使用 Microsoft Sysprep 创建的自定义规范进行了比较。

只有在 vSphere 模式以及 vSphere 4.1 软件中创建的池才支持 Sysprep。在 vSphere 4.0 或 VMware Infrastructure 3.5 软件中无法使用 Sysprep 自定义链接克隆桌面。

表 5–6 比较 QuickPrep 和 Microsoft Sysprep

QuickPrep	自定义规范 (Sysprep)
专为与 View Composer 配合使用而设计。 有关详细信息，请参阅第 77 页，“使用 QuickPrep 自定义链接克隆桌面”。	可以通过标准的 Microsoft Sysprep 工具创建。
为池中所有的链接克隆使用相同的本地计算机安全标识符 (Security Identifier, SID)。	为池中的每个链接克隆生成唯一的本地计算机 SID。
可以在关闭链接克隆之前，以及创建、刷新或重构链接克隆之后运行其他自定义脚本。	可以在用户首次登录时运行其他脚本。
将链接克隆计算机加入 Active Directory 域。	将链接克隆计算机加入 Active Directory 域。 **注意** 自定义规范必须将链接克隆计算机加入域（而不是工作组）中。
对于每个链接克隆，都要向 Active Directory 域帐户添加一个唯一 ID。	对于每个链接克隆，都要向 Active Directory 域帐户添加一个唯一 ID。
刷新链接克隆后不会生成新的 SID。通用 SID 将被保留。	自定义每个链接克隆时，均会生成一个新的 SID。在刷新操作过程中会保留唯一 SID，但在重构操作过程中不会保留。
重构链接克隆后不生成新的 SID。通用 SID 将被保留。	重构链接克隆后再次运行克隆，为虚拟机生成新的 SID。 有关详细信息，请参阅第 79 页，“重构使用 Sysprep 自定义的链接克隆”。
运行速度快于 Sysprep。	花费时间长于 QuickPrep。

如果使用 QuickPrep 或 Sysprep 自定义了链接克隆池，则在池中创建或重构桌面时，无法切换至其他自定义方法。

使用 QuickPrep 自定义链接克隆桌面

您可以通过使用 QuickPrep 系统工具，对父虚拟机创建的链接克隆桌面进行个性化。创建或重构链接克隆桌面时，View Composer 将执行 QuickPrep。

QuickPrep 通过以下几种方式自定义链接克隆桌面：

- 在您创建链接克隆池时为计算机指定一个名称。
- 在 Active Directory 中创建一个计算机帐户，将计算机添加到合适的域。
- 装载 View Composer 永久磁盘。Windows 用户配置文件将重定向到该磁盘。
- 将临时文件和页面文件重新定向到一个单独的磁盘。

这些步骤可能需要将链接克隆重新启动一次或多次。

QuickPrep 使用 KMS 卷许可证密钥激活 Windows 7 和 Windows Vista 链接克隆桌面。有关详细信息，请参阅第 59 页，“在链接克隆桌面上激活 Windows 7 和 Windows Vista”。

您可以自行创建脚本以进一步自定义链接克隆。QuickPrep 可以在预定义的时间运行两种类型的脚本：

- 在创建或重构链接克隆后
- 关闭链接克隆前

有关使用 QuickPrep 自定义脚本的指导原则和规则，请参阅第 78 页，“运行 QuickPrep 自定义脚本”。

注意 View Composer 需要使用域用户凭据，才能将链接克隆桌面加入 Active Directory 域中。有关详细信息，请参阅第 13 页，“为 View Composer 创建用户帐户”。

运行 QuickPrep 自定义脚本

利用 QuickPrep 工具，您可以创建脚本来自定义池中的链接克隆桌面。您可以将 QuickPrep 配置为在两个预定义的时间运行自定义脚本。

QuickPrep 脚本何时运行

同步后脚本会在创建、重构或重新平衡链接克隆后，且克隆的状态为 **[Ready（就绪）]** 时运行。关机脚本在链接克隆关闭之前运行。这些脚本在链接克隆的客户操作系统中运行。

QuickPrep 如何执行脚本

QuickPrep 进程使用 Windows `CreateProcess` API 调用来执行脚本。您的脚本可以调用任何 `CreateProcess` API 能够创建的进程。例如，`cmd`、`vbscript`、`exe`，以及可以和 API 协作的批文件进程。

具体说来，QuickPrep 将为脚本指定的路径作为第二个参数传递到 `CreateProcess` API，并将第一个参数设置为 `NULL`。

例如，如果脚本路径为 `c:\myscript.cmd`，其在 View Composer 日志文件的函数中显示为第二个参数：`CreateProcess(NULL,c:\myscript.cmd,...)`。

提供 QuickPrep 脚本的路径

当您创建链接克隆桌面池或编辑池的客户机自定义设置时，需要提供 QuickPrep 自定义脚本的路径。这些脚本必须位于父虚拟机中。您不能使用指向网络共享位置的 UNC 路径。

如果您使用需要解释程序才能执行脚本的脚本语言，则脚本路径必须以解释程序二进制文件的路径为开头。

例如，如果您指定 `C:\script\myvb.vbs` 作为 QuickPrep 自定义脚本的路径，View Composer Agent 将无法执行该脚本。您必须指定一个以解释程序二进制文件路径开始的路径：

```
C:\windows\system32\cscript.exe c:\script\myvb.vbs
```

QuickPrep 脚本超时限制

View Composer 会终止运行时间超过 20 秒的同步后脚本或关机脚本。如果脚本运行时间会超过 20 秒，您可以延长超时限制。有关详细信息，请参阅第 62 页，“延长 QuickPrep 自定义脚本的超时限制”。

或者，也可以使用您的脚本来启动其他执行长时间运行任务的脚本或进程。

QuickPrep 脚本帐户

QuickPrep 在配置运行 View Composer Agent 的帐户下运行脚本。默认情况下，这个帐户为 `SYSTEM`。

您可以使用 Windows 服务 (`services.msc`) 对话框更改 VMware View Composer Guest Agent Server 服务的登录属性，从而更改默认帐户。内部服务名称为 `vmware-viewcomposer-ga`。

QuickPrep 脚本日志

View Composer 日志中包含有关 QuickPrep 脚本的执行信息。日志中记录了执行的开始和结束时间以及输出或错误消息。日志位于 Windows `temp` 目录中：

```
C:\Windows\Temp\vmware-viewcomposer-ga-new.log
```

重构使用 Sysprep 自定义的链接克隆

如果要重构使用 Sysprep 自定义的链接克隆桌面，View Manager 会在重构操作系统磁盘后再次运行 Sysprep 自定义规范。此操作将为链接克隆虚拟机生成一个新的 SID。

如果生成新的 SID，则重构的链接克隆将像网络中的新计算机一样运行。某些软件程序（如系统管理工具）会根据 SID 识别受其管理的计算机。这些程序可能无法识别或定位链接克隆虚拟机。

此外，如果系统磁盘上安装了第三方软件，那么在重构完成后，自定义规范可能会为该软件重新生成 GUID。

首次运行自定义规范之前，重构操作会将链接克隆恢复为其初始状态。在这种状态下，链接克隆不具有本地计算机 SID 或任何安装在系统驱动器中的第三方软件的 GUID。重构链接克隆后，View Manager 必须运行 Sysprep 自定义规范。

链接克隆桌面池的存储大小

View Manager 提供了可帮助您确定链接克隆桌面池所需存储空间的高级指南。[Add Pool（添加池）] 向导会通过一个表来显示在创建池以及链接克隆逐渐增长的过程中，链接克隆磁盘存储需求的大体预估值。

存储大小表还会显示您选择用来存储操作系统磁盘、View Composer 永久磁盘以及副本的数据存储中的可用空间。您可以通过对比实际的可用空间和预估的链接克隆磁盘需求来确定使用哪些数据存储。

View Manager 使用的计算公式只能估算出大概的存储使用率。链接克隆的实际存储空间增长取决于诸多因素，例如：

- 分配给父虚拟机的内存容量
- 刷新操作的频率
- 客户操作系统页面文件的大小
- 是否将页面文件和临时文件重定向到一个单独的磁盘
- 是否配置了单独的 View Composer 永久磁盘
- 链接克隆桌面的负载，这主要由用户在客户操作系统上运行的应用程序类型决定

注意 在包含成百上千个链接克隆的部署中，您需要对其链接克隆池进行配置，使特定的数据存储组专供特定的 ESX 群集使用。请勿在所有数据存储中随机配置池，这样会导致多数或所有 ESX 主机必须访问多数或全部 LUN。

当过多的 ESX 主机试图向特定 LUN 中的链接克隆操作系统磁盘执行写入时，会出现争用问题，这会导致性能下降并影响可扩展性。有关在大型部署中规划数据存储的更多信息，请参阅《*VMware View 体系结构规划指南*》。

链接克隆池的大小调整原则

创建或编辑链接克隆桌面池时，**[Select Datastores（选择数据存储）]** 页面会显示一个关于存储大小的指示表。该表可帮助您决定为链接克隆磁盘选择哪些数据存储。

链接克隆磁盘的大小表

表 5-7 显示了在父虚拟机拥有 1 GB 内存和 10 GB 副本的情况下，一个拥有 10 台虚拟机的池可能显示的推荐存储大小示例。在此示例中，为操作系统磁盘和 View Composer 永久磁盘选择了不同的数据存储。

表 5–7 链接克隆磁盘大小表的示例

数据类型	选择的可用空间 (GB)	推荐的最小值 (GB)	50% 使用率 (GB)	推荐的最大值 (GB)
操作系统磁盘	184.23	40.00	80.00	130.00
永久磁盘	28.56	4.00	10.00	20.00

[Selected Free Space（选择的可用空间）] 列显示您为某个磁盘类型（如操作系统磁盘）所选的所有数据存储的总可用空间量。

[Min Recommended（推荐的最小值）] 列显示为一个池推荐的最小存储量。

[50% Utilization（50% 使用率）] 列显示当链接克隆磁盘增长到父虚拟机 50% 大小时推荐的存储量。

[Max Recommended（推荐的最大值）] 列显示当链接克隆磁盘接近父虚拟机大小时推荐的存储量。

如果将操作系统磁盘和永久磁盘存储在同一数据存储中，View Manager 会计算这两种磁盘类型的存储需求。**[Data Type（数据类型）]** 将显示为 **[Linked clones（链接克隆）]**，而不是某种特定的磁盘类型。

如果将 View Composer 副本存储在一个单独的数据存储中，该表还会显示针对副本的存储推荐并调整针对操作系统磁盘的存储推荐。

大小指导原则

该表提供了一般的指导原则。您在计算存储时还必须考虑影响链接克隆池实际存储增长的其他因素。

对于操作系统磁盘而言，您估计的大小具体取决于刷新和重构池的频率。

如果您刷新链接克隆池的频率介于一天一次和一周一次之间，请确保 **[Selected Free Space（选择的可用空间）]** 可以容纳介于 **[Min Recommended（推荐的最小值）]** 和 **[50% Utilization（50% 使用率）]** 预估值之间的存储使用量。

如果您很少刷新或重构池，链接克隆磁盘大小会持续增长。请确保 **[Selected Free Space（选择的可用空间）]** 可以容纳介于 **[50% Utilization（50% 使用率）]** 和 **[Max Recommended（推荐的最大值）]** 预估值之间的存储使用量。

对于永久磁盘而言，您估计的大小取决于用户在桌面上生成的 Windows 配置文件的数据量。刷新和重构操作不会影响永久磁盘。

View Manager 如何计算最小推荐大小

为计算出最小的操作系统磁盘推荐值，View Manager 将每个克隆初次创建及启动时消耗的存储量估计为其内存量的两倍。如果没有为克隆预留内存，则该克隆启动时，系统会为其创建一个 ESX 交换文件。客户操作系统页面文件的大小也会影响克隆操作系统磁盘的增长。

View Manager 在操作系统磁盘的最小推荐值中还包含了每个数据存储中的两个副本的空间。创建池时，View Manager 会创建一个副本。首次重构池时，View Manager 会在数据存储中创建第二个副本，然后将链接克隆绑定到新副本，如果没有其他克隆使用原始快照，View Composer 会同时删除第一个副本。重构操作过程中，数据存储的容量必须能存储两个副本。

默认情况下，副本使用 vSphere 精简部署，但为了使指导原则简单易算，View Manager 计为两个使用与父虚拟机所用空间量相同的副本。

为计算永久磁盘的最小推荐值，View Manager 将计算您在 [Add Pool（添加池）] 向导 **[View Composer Disks（View Composer 磁盘）]** 页面中所指定磁盘空间量的 20%。

注意 针对永久磁盘的计算是以静态阈值为基础的，以千兆字节为单位。例如，如果您指定的永久磁盘大小值介于 1024 MB 和 2047 MB 之间，View Manager 会按 1 GB 的永久磁盘大小进行计算。如果您指定的磁盘大小为 2048 MB，View Manager 会按 2 GB 的磁盘大小进行计算。

为计算出在单独数据存储上存储副本的推荐值，View Manager 会允许在数据存储上保留两个副本所用的空间量。计算最小及最大使用值时也会将该值计算在内。

有关详细信息，请参阅第 81 页，“链接克隆池的大小计算公式”。

大小指导原则和存储过载

在您预估出存储需求、选择数据存储并部署池之后，View Manager 会根据每个数据存储上的剩余空间和已有克隆数在不同数据存储中部署链接克隆虚拟机。

根据您在 [Add Pool（添加池）] 向导中 **[Select Datastores（选择数据存储）]** 页面上选择的存储过载选项，View Manager 会停止部署新克隆并为已有克隆预留可用空间。此行为可保证为数据存储中的每个桌面留出增长空间。

如果选择激进的存储过载级别，预估的存储需求可能会超出 **[Selected Free Space（已选可用空间）]** 列中显示的容量。存储过载级别会影响 View Manager 在一个数据存储中实际创建的虚拟机的数量。

有关详细信息，请参阅第 82 页，“设置链接克隆桌面的存储过载级别”。

链接克隆池的大小计算公式

利用存储空间大小计算公式，您可以为针对操作系统磁盘、View Composer 永久磁盘和副本而选择的数据存储估算链接克隆磁盘的大小（相对于可用空间）。

存储大小计算公式

表 5‑8 显示了在创建池时以及链接克隆桌面逐渐增长过程中计算链接克隆磁盘预计大小的公式。这些公式会将随克隆一起存储在数据存储中的副本所占的磁盘空间计算在内。

如果您编辑已有池或将副本存储在单独的数据存储中，View Manager 会使用不同的大小计算公式。请参阅第 81 页，“编辑池或在单独数据存储中存储副本时创建链接克隆的大小计算公式”。

表 5‑8 选定数据存储中链接克隆磁盘存储大小的计算公式

数据类型	选择的可用空间 (GB)	推荐的最小值 (GB)	50% 使用率 (GB)	推荐的最大值 (GB)
操作系统磁盘	选定数据存储中的可用空间	虚拟机数量 * (2 * 虚拟机内存) + (2 * 副本磁盘)	虚拟机数量 * (副本磁盘的 50% + 虚拟机内存) + (2 * 副本磁盘)	虚拟机数量 * (副本磁盘的 100% + 虚拟机内存) + (2 * 副本磁盘)
永久磁盘	选定数据存储中的可用空间	虚拟机数量 * 永久磁盘的 20%	虚拟机数量 * 永久磁盘的 50%	虚拟机数量 * 永久磁盘的 100%

存储大小预估示例

在这个示例中，为父虚拟机配置的内存为 1 GB。父虚拟机的磁盘大小为 10 GB 链接克隆池中创建了 10 个桌面。永久磁盘的大小配置为 2048 MB。

操作系统配置在一个当前有 184.23 GB 可用空间的数据存储中。永久磁盘配置在另一个有 28.56 GB 可用空间的数据存储中。

表 5‑9 显示了大小计算公式如何计算示例链接克隆池的预估空间需求。

表 5‑9 部署在选定数据存储中的链接克隆磁盘的大小预估示例

数据类型	选择的可用空间 (GB)	推荐的最小值 (GB)	50% 使用率 (GB)	推荐的最大值 (GB)
操作系统磁盘	184.23	10 * (2 * 1 GB) + (2 * 10 GB) = 40.00	10 * (10 GB 的 50% + 1 GB) + (2 *10 GB) = 80.00	10 * (10 GB 的 100% + 1 GB) + (2 * 10 GB) = 130.00
永久磁盘	28.56	10 * (2 GB 的 20%) = 4.00	10 * (2 GB 的 50%) = 10.00	10 * (2 GB 的 100%) = 20.00

编辑池或在单独数据存储中存储副本时创建链接克隆的大小计算公式

当您编辑已有链接克隆池或在单独的数据存储中存储副本时，View Manager 所用计算公式与您第一次创建池时所用的公式不同。

如果您编辑现有池，为该池选择数据存储，View Composer 会在选定数据存储中创建新克隆。新克隆会被绑定到现有快照并使用现有副本磁盘。不会创建新副本。

如果您将副本存储在一个单独的数据存储中，其他选定的数据存储会专供链接克隆磁盘使用。

在这些情况下，View Manager 计算链接克隆磁盘的推荐存储空间时不会将副本空间计算在内。

表 5‑10 显示了编辑池或在单独的数据存储中存储副本时计算链接克隆磁盘的预估大小所用的公式。

表 5–10 编辑池或在单独的数据存储中存储副本时链接克隆存储的大小计算公式

数据类型	选择的可用空间 (GB)	推荐的最小值 (GB)	50% 使用率 (GB)	推荐的最大值 (GB)
操作系统磁盘	选定数据存储中的可用空间	虚拟机数量 * (2 * 虚拟机内存)	虚拟机数量 * (副本磁盘的 50% + 虚拟机内存)	虚拟机数量 * (副本磁盘的 100% + 虚拟机内存)
永久磁盘	选定数据存储中的可用空间	虚拟机数量 * 永久磁盘的 20%	虚拟机数量 * 永久磁盘的 50%	虚拟机数量 * 永久磁盘的 100%

编辑池或在单独的数据存储中存储副本时的存储大小预估示例

在这个示例中，为父虚拟机配置的内存为 1 GB。父虚拟机的磁盘大小为 10 GB 链接克隆池中创建了 10 个桌面。永久磁盘的大小配置为 2048 MB。

操作系统配置在一个当前有 184.23 GB 可用空间的数据存储中。永久磁盘配置在另一个有 28.56 GB 可用空间的数据存储中。

表 5–11 显示了大小计算公式如何计算示例链接克隆池的预估存储需求。

表 5–11 编辑池或在单独的数据存储中存储副本时链接克隆磁盘的大小预估计示例

数据类型	选择的可用空间 (GB)	推荐的最小值 (GB)	50% 使用率 (GB)	推荐的最大值 (GB)
操作系统磁盘	184.23	10 * (2 * 1 GB) = 20.00	10 * (10 GB 的 50% + 1 GB) = 60.00	10 * (10 GB 的 100% + 1 GB) = 110.00
永久磁盘	28.56	10 * (2 GB 的 20%) = 4.00	10 * (2 GB 的 50%) = 10.00	10 * (2 GB 的 100%) = 20.00

设置链接克隆桌面的存储过载级别

使用存储过载功能可以控制 View Manager 在数据存储中创建链接克隆桌面时的激进程度。利用此功能，您创建的链接克隆的逻辑总大小可以超过数据存储的物理存储限制。

此功能仅适用于链接克隆池。

存储过载级别将计算在每个克隆都是完整虚拟机的情况下，克隆所用的超出数据存储物理大小的存储量。有关详细信息，请参阅第 83 页，“链接克隆桌面的存储过载”。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 创建新桌面池或编辑已有池时，请导航至 [Select Datastores（选择数据存储）] 页面。

选项	操作
新桌面池	a 单击 **[Add（添加）]**。 b 按照 [Add Pool（添加池）] 向导中的提示操作，直到 [Select Datastores（选择数据存储）] 页面出现。
已有桌面池	a 选择链接克隆池，然后单击 **[Edit（编辑）]**。 b 单击 **[vCenter Settings（vCenter 设置）]** 选项卡。

3 在 [Select Datastores（选择数据存储）] 页面上，选择存储过载级别。

选项	描述
None（无）	不允许存储过载。
Conservative（保守）	数据存储大小的 4 倍。这是默认级别。

选项	描述
Moderate（中等）	数据存储大小的 7 倍。
Aggressive（激进）	数据存储大小的 15 倍。

4 单击 **[Done（完成）]**。

5 单击 **[Finish（完成）]**。

链接克隆桌面的存储过载

通过使用存储过载功能，您在数据存储中存放的链接克隆桌面的数量可以超过其能存放的完整虚拟机桌面的数量，从而降低了存储成本。链接克隆可以使用容量为数据存储物理容量若干倍的逻辑存储空间。

此功能可帮助您选择一个允许您过量分配数据存储容量，并为 View Manager 创建的链接克隆设置数量限制的存储级别。您可以避免由于部署过于保守而浪费存储，也可以避免链接克隆用尽磁盘空间并导致桌面应用程序失败。

例如，如果每个虚拟机的大小为 10 GB，则在 100 GB 的数据存储中，最多可以创建 10 个完整虚拟机。如果您从 10 GB 父虚拟机创建链接克隆，则每个克隆的大小都要远远小于 10 GB。

如果您设置保守的过载级别，按每个克隆的大小与父虚拟机相同计算，View Manager 允许克隆使用的存储空间将是数据存储物理大小的 4 倍。在 100 GB 的数据存储中，如果父虚拟机大小为 10 GB，View Manager 可部署大约 40 个链接克隆。即使数据存储中还有可用空间，View Manager 也不会部署更多克隆。此限制为现有克隆的增长保留了空间。

表 5-12 显示了您可以设置的存储过载级别。

表 5–12 存储过载级别

选项	存储过载级别
None（无）	不允许存储过载。
Conservative（保守）	数据存储大小的 4 倍。这是默认级别。
Moderate（中等）	数据存储大小的 7 倍。
Aggressive（激进）	数据存储大小的 15 倍。

存储过载级别为确定存储容量提供了高级指南。要确定最佳级别，请监视环境中链接克隆的增长情况。

如果操作系统磁盘不可能增至最大，请设置激进级别。设置激进的过载级别时，您需要密切关注。要确保链接克隆不会用尽磁盘空间，您可以定期刷新或重新平衡桌面池，将链接克隆的操作系统数据减小到其原始大小。

例如，如果将浮动分配桌面池中的桌面设置为在注销后删除或刷新，就应当为此浮动分配桌面池设置激进的过载级别。

您可以为不同类型的数据存储指定不同的存储过载级别，以满足每个数据存储的不同吞吐量级别要求。例如，NAS 数据存储的设置可以不同于 SAN 数据存储。

将 View Composer 副本和链接克隆存储在单独的数据存储中

您可以将 View Composer 副本和链接克隆分别存放在具有不同性能特征的数据存储中。这种灵活配置可加快密集操作（例如一次部署多个链接克隆，或者运行防病毒扫描）的速度。

例如，您可以将副本虚拟机存储在以固态磁盘作为后端的数据存储中。固态磁盘具有低存储容量和高读取性能，通常支持 20,000 I/O 每秒 (IOPS) 的速度。View Composer 只为每个 ESX 群集上的每个 View Composer 基础映像快照创建一份副本，因此副本不需要太多存储空间。同时在多个链接克隆上执行某一任务时，固态磁盘可提高 ESX 读取副本操作系统磁盘的速度。

您可以将链接克隆存储在以传统旋转介质作为后端的数据存储中。这种磁盘性能较低，通常支持 200 IOPS。但这种磁盘价格低廉，并具有高存储容量，因此适合存储大型池中的大量链接克隆。ESX 不需要在链接克隆上同时执行多个密集读取操作。

以这种方式配置副本和链接克隆可以降低一次创建大量链接克隆时出现的 I/O 风暴所带来的影响。例如，如果您部署一个具有“注销后删除桌面”策略的浮动分配池，并且用户在同一时间开始工作，那么 View Manager 必须同时为他们部署新桌面。

重要事项 此功能面向由提供高性能磁盘解决方案的供应商所提供的特定存储配置。如果您的存储硬件不支持高读取性能，请不要将副本存储在单独的数据存储中。

将池中的副本和链接克隆存储在单独的数据存储中时，必须遵循以下特定要求：

- 您只能为一个池指定一个单独的副本数据存储。
- 如果副本数据存储是共享存储，则必须能够从群集中的所有 ESX 主机上访问它。
- 如果链接克隆数据存储是共享存储，则副本数据存储也必须是共享的。只有当您将所有链接克隆配置在同一 ESX 主机上的本地数据存储时，副本才能驻留在本地数据存储中。

此功能只可在 vSphere 模式中使用。链接克隆必须部署在运行 ESX 4 或更高版本的主机或群集上。

在单独的数据存储或共享数据存储中存储副本时的可用性问题

您可以将 View Composer 副本存储在一个单独的数据存储中，或者与链接克隆虚拟机存储在相同的数据存储中。这些配置会以不同方式影响池的可用性。

将副本与链接克隆存储在相同的数据存储中时，为增强可用性，View Composer 会在每个数据存储中创建一个单独的副本。如果某一数据存储不可用，则只有该数据存储上的链接克隆才会受到影响，其他数据存储中的链接克隆仍可继续运行。

如果将副本存储在一个单独的数据存储中，那么池中的所有链接克隆都将与该数据存储中的副本绑定。如果该数据存储不可用，整个池都将不可用。

为增强链接克隆桌面的可用性，您可以为存储副本的数据存储配置一个高可用性解决方案。

链接克隆桌面的数据磁盘

View Composer 可创建多个数据磁盘来存储链接克隆桌面的组件。

操作系统磁盘

View Composer 会为每个链接克隆创建一个操作系统磁盘。该磁盘将存储克隆保持与基础映像链接及作为唯一桌面运行所需的系统数据。

QuickPrep 配置数据磁盘

View Composer 在创建操作系统磁盘的同时会创建一个辅助磁盘。辅助磁盘将存储在刷新和重构操作时必须保留的 QuickPrep 配置数据和其他与操作系统相关的数据。该磁盘的容量较小，通常约为 20 MB。无论您使用 QuickPrep 还是 Sysprep 来自定义桌面，都会创建此磁盘。

如果您配置单独的 View Composer 永久磁盘来存储用户配置文件，则与每个链接克隆相关联的磁盘有三个：操作系统磁盘、辅助桌面磁盘以及 View Composer 永久磁盘。

辅助桌面磁盘与操作系统磁盘存储在同一数据存储内。您不能配置该磁盘。

View Composer 永久磁盘

在专用分配池中，您可以配置单独的 View Composer 永久磁盘来存储 Windows 用户配置文件数据。该磁盘不是必需的。

您可以使用单独的永久磁盘保留用户数据和设置。View Composer 刷新、重构和重新平衡操作不会影响永久磁盘。您可以将永久磁盘从一个链接克隆中分离，然后将其附加到另一个链接克隆。

如果不配置单独的永久磁盘，Windows 配置文件将存储在操作系统磁盘中。用户数据和设置在刷新、重构和重新平衡期间将被移除。

您可以将永久磁盘与操作系统磁盘存储在同一数据存储内，也可以将其存储在不同的数据存储中。

一次性数据磁盘

创建链接克隆池时，您可以配置一个单独的非永久磁盘，用来存储客户操作系统在用户会话期间生成的页面文件和临时文件。您必须指定磁盘大小（以 MB 为单位）。

该磁盘不是必需的。

链接克隆关闭后，View Manager 将删除一次性文件。链接克隆的大小在用户与其桌面交互过程中会增长。使用一次性文件可以减缓链接克隆的增长速度，从而节省存储空间。

一次性数据磁盘与操作系统磁盘存储在同一数据存储中。

手动桌面池

为创建手动桌面池，View Manager 会从现有的桌面源部署桌面。对于池中每个桌面，您需要选择一个单独的桌面源来向客户端交付 View 访问。

View Manager 可以在手动池中使用几种类型的桌面源：

- vCenter Server 管理的虚拟机
- 在 VMware Server 或其他虚拟化平台上运行的虚拟机
- 物理机
- HP 刀片 PC

用于创建手动桌面池的工作表

当您创建手动桌面池时，View Administrator 的 [Add Pool（添加池）] 向导会提示您配置特定选项。您可以使用此工作表在创建池之前准备配置选项。

您可以打印此工作表，并记下您要在运行 [Add Pool（添加池）] 向导时指定的值。

注意 在手动池中，您必须准备每个桌面源才能交付 View 桌面访问。View Agent 必须安装并运行在每个桌面源上。

表 5–13 工作表：用于创建手动桌面池的配置选项

选项	描述	在此填写您要指定的值
User assignment（用户分配）	选择用户分配类型： ■ 在专用分配池中，每个用户会分配给一个桌面。用户每次登录时会收到相同的桌面。 ■ 在浮动分配池中，用户每次登录时都会接收到不同的桌面。 有关详细信息，请参阅第 91 页，“桌面池中的用户分配”。	
Desktop Sources（桌面源）	您要用作池中的 View 桌面的虚拟机或物理机。 1 确定您要使用的桌面源类型。可以使用受 vCenter Server 管理的虚拟机或未受管的虚拟机、物理机以及刀片 PC。 2 准备好要包含在池中的 vCenter Server 虚拟机或未受管虚拟机、物理机以及刀片 PC 的列表。 要在桌面源（未受管虚拟机、物理机或刀片 PC）中使用 PCoIP，必须使用 Teradici 硬件。	

表 5–13 工作表：用于创建手动桌面池的配置选项 （续）

选项	描述	在此填写您要指定的值
vCenter Server	用来管理桌面的 vCenter Server。 仅当桌面源是受 vCenter Server 管理的虚拟机时，才会显示此选项。	
Pool ID（池 ID）	用户登录时看到的池名称，用于在 View Administrator 中标识池。 如果您的环境中运行了多个 vCenter Server，应确保其他 vCenter Server 没有使用同一个池 ID。	
Pool Settings（池设置）	这些设置用于确定桌面状态、虚拟机处于未使用状态时的电源状态、显示协议、Adobe Flash 质量等。 有关详细信息，请参阅第 96 页，“桌面和池的设置”。 有关适用于手动池的设置列表，请参阅第 88 页，“手动池的桌面设置”。	

创建手动桌面池

您可以创建一个通过现有虚拟机、物理机和 HP 刀片 PC 部署桌面的手动桌面池。您必须选择可构成池中 View 桌面的桌面源。

对于由 vCenter Server 管理桌面的手动池，View Manager 会确保一个备用桌面保持开启状态以供用户连接。无论应用哪种电源策略，备用桌面都会处于开启状态。

前提条件

- 准备桌面源来交付 View 桌面访问。在手动池中，您必须分别准备每个桌面源。View Agent 必须安装并运行在每个桌面源上。

  要准备受 vCenter Server 管理的虚拟机，请参阅第 41 页，第 4 章“创建和准备虚拟机”。

  要准备未受管虚拟机、物理机或刀片 PC，请参阅第 37 页，第 3 章“准备未受管的桌面源”。
- 收集您在创建池时必须提供的配置信息。请参阅第 85 页，“用于创建手动桌面池的工作表”。
- 确定如何配置电源设置、显示协议、Adobe Flash 质量及其他设置。请参阅第 96 页，“桌面和池的设置”。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 单击 **[Add（添加）]**。

3 选择 **[Manual Pool（手动池）]**。

4 按照向导中的提示创建池。

  使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称，您可以直接返回至已完成的任意向导页面。

要查看添加到池的桌面，您可以在 View Administrator 中单击 **[Inventory（清单）] > [Desktops（桌面）]**。

下一步

授予用户访问池的权限。请参阅第 103 页，“向桌面池添加授权”。

创建包含一个桌面的手动池

当用户需要一个唯一的专用桌面，或者多个用户需要在不同时间访问某个使用单一主机许可证的高成本应用程序时，您可以创建一个包含单个桌面的池。

通过创建手动桌面池并选择单个桌面源，您可以将单个 View 桌面部署在其专有的池中。

要模拟可由多个用户共享的物理机，可为具有池访问授权的用户指定浮动分配。

无论您使用专用分配还是浮动分配来配置单一桌面池，电源操作均由会话管理启动。虚拟机在用户请求桌面时开机，并在用户注销时关机或挂起。

如果您配置 **[Ensure desktops are always powered on（确保桌面始终开启）]** 策略，虚拟机将保持开机状态。如果用户关闭虚拟机，它将立即重新启动。

前提条件

- 准备桌面源来交付 View 桌面访问。View Agent 必须安装并运行在该桌面源上。

  要准备受 vCenter Server 管理的虚拟机，请参阅第 41 页，第 4 章“创建和准备虚拟机”。

  要准备未受管虚拟机、物理机或刀片 PC，请参阅第 37 页，第 3 章“准备未受管的桌面源”。

- 收集您在创建手动池时必须提供的配置信息。请参阅第 85 页，“用于创建手动桌面池的工作表”。
- 确定如何配置电源设置、显示协议、Adobe Flash 质量及其他设置。请参阅第 96 页，“桌面和池的设置”。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 单击 **[Add（添加）]**。

3 选择 **[Manual Pool（手动池）]**。

4 选择用户分配类型。

选项	描述
Dedicated Assignment（专用分配）	桌面分配给一个用户。只有该用户才可以登录此桌面。
Floating Assignment（浮动分配）	桌面由具有池授权的所有用户分享。只要没有用户正在使用，任何得到授权的用户均可以登录此桌面。

5 在 [Add vCenter Virtual Machines（添加 vCenter 虚拟机）] 或 [Add Machines（添加计算机）] 页面上，为您的桌面选择桌面源。

6 按照向导中的提示创建池。

  使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称，您可以直接返回至已完成的任意向导页面。

要查看所创建的桌面，您可以在 View Administrator 中单击 **[Inventory（清单）] > [Desktops（桌面）]**。

下一步

授予用户访问池的权限。请参阅第 103 页，“向桌面池添加授权”。

手动池的桌面设置

配置手动池时，您必须指定桌面和池的设置。并非所有设置都适用于所有类型的手动池。

表 5-14 列出了适用于通过以下属性配置的手动桌面池的设置：

- Dedicated user assignments（专用用户分配）
- Floating user assignments（浮动用户分配）
- Managed desktop sources (vCenter Server virtual machines)（受管的桌面源（vCenter Server 虚拟机））
- Unmanaged desktop sources（未受管的桌面源）

这些设置仅适用于包含单个桌面的手动池。

有关每种桌面设置的描述，请参阅第 96 页，“桌面和池的设置”。

表 5–14 手动桌面池的设置

设置	受管的专用分配手动池	受管的浮动分配手动池	未受管的专用分配手动池	未受管的浮动分配手动池
State（状态）	是	是	是	是
Connection Server restrictions（Connection Server 限制）	是	是	是	是
Remote desktop power policy（远程桌面电源策略）	是	是		
Automatic logoff after disconnect（断开连接后自动注销）	是	是	是	是
Allow users to reset their desktop（允许用户重置桌面）	是	是		
Allow multiple sessions per user（允许每个用户多个会话）		是		是
Default display protocol（默认显示协议）	是	是	是 要在不受 vCenter Server 管理的桌面源中使用 PCoIP，您必须在该桌面源上安装 Teradici 硬件。	是 要在不受 vCenter Server 管理的桌面源中使用 PCoIP，您必须在该桌面源上安装 Teradici 硬件。
Allow users to choose protocol（允许用户选择协议）	是	是	是	是
Max number of monitors（显示器最大数量）	是	是		
Max resolution of any one monitor（任意一台显示器的最大分辨率）	是	是		

表 5–14 手动桌面池的设置（续）

设置	受管的专用分配手动池	受管的浮动分配手动池	未受管的专用分配手动池	未受管的浮动分配手动池
Adobe Flash quality（Adobe Flash 质量）	是	是	是	是
Adobe Flash throttling（Adobe Flash 调节）	是	是	是	是

Microsoft 终端服务池

您可以使用 Microsoft 终端服务器将终端服务会话作为桌面提供给 View 客户端。View Manager 管理终端服务会话的方式与管理其他 View 桌面的方式相同。

终端服务池可以包含由一个或多个终端服务器提供服务的多个桌面源。一个终端服务器桌面源可交付多个 View 桌面。

View Manager 通过将连接请求定向到活动会话数最少的终端服务器来为池中的终端服务器提供负载平衡。

您可以将整个终端服务池授权给用户或用户组。

您应当部署一个漫游配置文件解决方案，以便将用户设置和数据传播到用户当前访问的桌面。

注意 终端服务池仅支持 RDP 显示协议。

创建 Microsoft 终端服务池

您可以创建通过终端服务器桌面源部署桌面的 Microsoft 终端服务池。您必须选择构成池中 View 桌面的桌面源。

前提条件

- 准备终端服务器桌面源来交付 View 桌面访问。View Agent 必须安装并运行在每个桌面源上。请参阅第 37 页，第 3 章“准备未受管的桌面源”。
- 制作您要包含在池中的终端服务器桌面源列表。
- 确定如何配置桌面设置。请参阅第 90 页，“Microsoft 终端服务池的桌面设置”。有关每种桌面设置的描述，请参阅第 96 页，“桌面和池的设置”。
- 提供用户登录时看到的，可在 View Administrator 中标识池的池 ID。如果您的环境中运行了多个 vCenter Server，应确保其他 vCenter Server 没有使用同一个池 ID。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 单击 **[Add（添加）]**。

3 选择 **[Microsoft Terminal Services Desktop Pool（Microsoft 终端服务桌面池）]**。

4 按照向导中的提示创建池。

  需要使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称，可以直接返回至已完成的任意向导页面。

要查看添加到池的桌面，您可以在 View Administrator 中单击 **[Inventory（清单）] > [Desktops（桌面）]**。

下一步

授予用户访问池的权限。请参阅第 103 页，“向桌面池添加授权”。

Microsoft 终端服务池的桌面设置

配置 Microsoft 终端服务池时，您必须指定桌面和池的设置。并非所有设置都适用于所有类型的终端服务池。

表 5–15 列出了适用于终端服务池的设置。

有关每种桌面设置的描述，请参阅第 96 页，“桌面和池的设置”。

表 5–15 终端服务池设置

设置	Microsoft 终端服务池
State（状态）	是
Connection Server restrictions（Connection Server 限制）	是
Automatic logoff after disconnect（断开连接后自动注销）	是
Default display protocol（默认显示协议）	终端服务池仅支持 RDP 显示协议。
Adobe Flash quality（Adobe Flash 质量）	是
Adobe Flash throttling（Adobe Flash 调节）	是

在终端服务会话中配置 Internet Explorer 中的 Adobe Flash 调节

要确保 Internet Explorer 在终端服务会话中可以使用 Adobe Flash 调节功能，用户必须启用第三方浏览器扩展名。

步骤

1 启动 View Client 并登录到一个用户的桌面。

2 在 Internet Explorer 中，单击 **[Tools（工具）] > [Internet Options（Internet 选项）]**。

3 单击 **[Advanced（高级）]** 选项卡，选择 **[Enable third-party browser extensions（启用第三方浏览器扩展）]**，单击 **[OK（确定）]**。

4 重新启动 Internet Explorer。

部署桌面池

创建桌面池时，您需要选择配置选项，从而确定池的管理方式，以及用户与桌面的交互方式。

- 桌面池中的用户分配第 91 页，

  您可以对桌面池进行配置，以便用户对池中的桌面具有专用分配或浮动分配。对于包含完整虚拟机的自动池、自动链接克隆池以及手动池，您必须选择一个用户分配。

- 手动命名桌面或提供命名模式第 91 页，

  通过手动指定桌面名称列表，或是提供命名模式以及要在池中部署的桌面数量，您可以在自动池中部署桌面。这两种方法各有优势。

- 手动自定义桌面第 95 页，

  创建自动池后，您可以在不重新分配所有权的情况下自定义特定的桌面。通过在维护模式下启动桌面，您可以先修改和测试桌面，然后再将它们发布给分配的用户，或是提供给池中具有授权的所有用户使用。

- 桌面和池的设置第 96 页，

  在配置包含完整虚拟机的自动池、链接克隆桌面池、手动桌面池以及 Microsoft 终端服务池时，您必须指定桌面和池的设置。并非所有设置都适用于所有类型的桌面池。

桌面池中的用户分配

您可以对桌面池进行配置，以便用户对池中的桌面具有专用分配或浮动分配。对于包含完整虚拟机的自动池、自动链接克隆池以及手动池，您必须选择一个用户分配。

在专用分配中，View Manager 会将每个授权的用户分配到池中一个桌面。当用户连接到池时，将始终登录同一桌面。系统会保存会话之间的用户设置和数据。池中的其他用户均不能访问该桌面。

在浮动分配中，View Manager 会将池中的桌面动态分配给授权的用户。用户每次登录时将连接到不同的桌面，当用户注销后，桌面将返回到池中。

您可以将浮动分配桌面配置为在用户注销后删除。通过自动删除，可以每次只保留您需要的虚拟机数量。您只可以在通过桌面命名模式和桌面总数部署的自动池中使用自动删除功能。

浮动分配桌面可以降低软件许可成本。

手动命名桌面或提供命名模式

通过手动指定桌面名称列表，或是提供命名模式以及要在池中部署的桌面数量，您可以在自动池中部署桌面。这两种方法各有优势。

如果通过指定列表来命名桌面，您可以使用所在公司的命名方案，并且可以将每个桌面名称与一个用户相关联。

如果您提供了命名模式，View Manager 可以根据用户的需要动态创建和分配桌面。

您必须使用这两种命名方法中的一种来部署包含完整虚拟机或链接克隆的自动池。

表 5‑16 对两种命名方法进行了比较，显示了两种方法对桌面池的创建和管理方式的影响。

表 5‑16 手动命名桌面或提供桌面命名模式

功能	提供桌面命名模式	手动命名桌面
桌面名称	View Manager 将生成桌面名称。 您要提供一个命名模式。View Manager 添加一个唯一编号来标识各个桌面。 有关详细信息，请参阅第 93 页，“为自动桌面池使用命名模式”。	您要指定一个桌面名称列表。 在专用分配池中，您可以通过列出用户名和桌面名称将用户与桌面配对。 有关详细信息，请参阅第 92 页，“指定桌面名称列表”。
池大小	您要指定桌面的最大数量。	您指定的桌面名称列表确定了桌面的数量。
将桌面添加到池中	您可以增加池大小的上限。	您可以将桌面名称添加到列表中。 有关详细信息，请参阅第 163 页，“将桌面添加到通过名称列表部署的自动池中”。
按需部署	可用。 View Manager 可以在用户首次登录时为其创建和部署桌面。 View Manager 还可以在您创建池时创建和部署所有桌面。	不可用。 View Manager 在创建池时将创建和部署您在列表中指定的所有桌面。
初始自定义	可用。 部署桌面后，View Manager 可以运行您选择的自定义规范。	可用。 部署桌面后，View Manager 可以运行您选择的自定义规范。
手动自定义专用桌面	要自定义桌面并将其访问权返回给用户，您必须移除并重新分配每个桌面的所有权。根据是否在首次登录时分配桌面，您可能需要将这些步骤执行两次。您不能在维护模式下启动桌面。创建池后，您可以手动将桌面置于维护模式。	您可以在不重新分配所有权的情况下对桌面进行自定义和测试。 创建池时，您可以将所有桌面在维护模式下启动，以阻止用户访问桌面。您可以自定义这些桌面，然后退出维护模式，将访问权返回给用户。 有关详细信息，请参阅第 95 页，“手动自定义桌面”。

表 5–16 手动命名桌面或提供桌面命名模式 （续）

功能	提供桌面命名模式	手动命名桌面
动态或固定的池大小	动态。 如果从专用分配池中的某个桌面移除用户分配，该桌面将被返回到可用的桌面池。 如果您在浮动分配池中选择注销后删除桌面，那么根据活动用户会话的数量，池大小可能会增大或缩小。	固定。 池中包含的桌面数量是您在桌面名称列表中提供的。 如果您手动命名桌面，则不能选择 **[Delete desktop on logoff（注销后删除桌面）]** 设置。
备用桌面	您可以指定一些备用桌面，View Manager 会使这些桌面保持开机状态，以供新用户使用。 View Manager 会创建新的桌面以维持指定的数量。池的大小达到上限后，View Manager 将停止创建备用桌面。 View Manager 将使备用桌面保持开机状态，即便池的电源策略为 **[Power off（关机）]** 或 **[Suspend（挂起）]**，或者您并没有设置电源策略。	您可以指定一些备用桌面，View Manager 会使这些桌面保持开机状态，以供新用户使用。 View Manager 不会创建新的备用桌面来维持指定的数量。 View Manager 将使备用桌面保持开机状态，即便池的电源策略为 **[Power off（关机）]** 或 **[Suspend（挂起）]**，或者您并没有设置电源策略。
用户分配	您可以为专用分配池和浮动分配池使用命名模式。	您可以为专用分配池和浮动分配池指定桌面名称。 **注意** 在浮动分配池中，您不能将用户名与桌面名称相关联。桌面不会专供关联的用户使用。在浮动分配池中，当前未处于使用状态的所有桌面均可供登录的用户访问。

指定桌面名称列表

您可以通过手动指定桌面名称列表来部署自动桌面池。此命名方法允许您使用自己公司的命名约定来标识池中的桌面。

如果您明确指定桌面名称，那么用户登录其桌面时将看到基于其所在公司组织的熟悉名称。

按照以下指南手动指定桌面名称：

- 将每个桌面名称键入单独的一行中。
- 桌面名称最多可以包含 15 个字母数字字符。
- 可以为每个桌面条目添加一个用户名。使用逗号来分隔用户名与桌面名称。

在此示例中指定了两个桌面。第二个桌面与一个用户相关联：

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

注意 在浮动分配池中，您不能将用户名与桌面名称相关联。桌面不会专供关联的用户使用。在浮动分配池中，当前未处于使用状态的所有桌面均可供登录的用户访问。

前提条件

确保每个桌面名称都是唯一的。不能使用 vCenter Server 中现有虚拟机的名称。

步骤

1 创建一个包含桌面名称列表的文本文件。

  如果要创建仅包含几个桌面的池，您可以直接在 [Add Pool（添加池）] 向导中键入桌面名称，而不必创建单独的文本文件。

2 在 View Administrator 中，启动 [Add Pool（添加池）] 向导，开始创建自动桌面池。

3 在 [Provisioning Settings（部署设置）] 页面上，选择 **[Specify names manually（手动指定名称）]**，然后单击 **[Enter names（输入名称）]**。

4 将您的桌面名称列表复制到 [Enter Desktop Names（输入桌面名称）] 页面中，然后单击 **[Next（下一步）]**。

 [Enter Desktop Names（输入桌面名称）] 向导将显示桌面列表，并用红色的 **[X]** 来表明验证错误。

5 纠正无效的桌面名称。

 a 将鼠标放置在无效名称上方，页面底部会显示相关的错误消息。

 b 单击 **[Back（返回）]**。

 c 编辑该错误名称，然后单击 **[Next（下一步）]**。

6 单击 **[Finish（完成）]**。

7 （可选）选择 **[Start desktops in maintenance mode（在维护模式下启动桌面）]**。

 利用此选项，您可以先自定义桌面，然后再允许用户登录和使用桌面。

8 按照向导中的提示完成桌面池的创建。

View Manager 将为列表中的每个名称创建一个桌面。对于包含桌面和用户名的条目，View Manager 会将该桌面分配给条目中的用户。

创建池之后，您可以导入另一个包含其他桌面名称和用户的列表文件，从而添加更多桌面。

为自动桌面池使用命名模式

您可以通过提供命名模式和要在池中部署的桌面总数在池中部署桌面。默认情况下，View Manager 会使用您提供的模式作为所有桌面名称的前缀，并后加一个唯一的编号来标识各个桌面。

桌面名称中的命名模式长度

包括命名模式和自动生成的编号在内，桌面名称的长度不能超过 15 个字符。

表 5–17 桌面名称中的命名模式最大长度

如果在池中设置以下数量的桌面	最大前缀长度如下
1-99	13 个字符
100-999	12 个字符
1,000 或更多	11 个字符

包含固定长度令牌的名称具有不同的长度限制。请参阅第 93 页，“使用固定长度令牌时的命名模式长度”。

在桌面名称中使用令牌

通过使用令牌，您可以将自动生成的编号放置在名称中的任何位置。当您键入池名称时，需要在大括号中键入 **n** 来指定令牌。

例如：**amber-{n}-desktop**

View Manager 创建桌面时，View Manager 将把 **{n}** 替换为一个唯一编号。

您可以通过键入 **{n:fixed=*<位数>*}** 来生成一个固定长度的令牌。

View Manager 会将该令牌替换为包含指定位数的编号。

例如，如果您键入 **amber-{n:fixed=3}**，View Manager 将把 **{n:fixed=3}** 替换为一个三位数的编号，从而创建以下桌面名称：**amber-001**、**amber-002** 和 **amber-003** 等。

使用固定长度令牌时的命名模式长度

包括命名模式和令牌位数在内，包含固定长度令牌的名称的长度不能超过 15 个字符。

表 5–18 使用固定长度令牌时的命名模式最大长度

固定长度的令牌	命名模式的最大长度
{n:fixed=1}	14 个字符
{n:fixed=2}	13 个字符
{n:fixed=3}	12 个字符

桌面命名示例

此示例显示了如何创建两个使用相同桌面名称，但各有一组不同编号的自动桌面池。此示例中使用的策略实现了具体的用户目标并展示了桌面命名方式的灵活性。

我们的目标是创建两个具有相同命名约定的池，如 VDIABC-*XX*，其中 *XX* 代表编号。每个池具有一组不同的顺序编号。例如，第一个池包含的桌面可能是 VDIABC-01 到 VDIABC-10，第二个池包含的桌面可能是 VDIABC-11 到 VDIABC-20。

您可以使用任意一种桌面命名方法来实现此目标。

- 要一次创建固定数目的桌面集，可手动指定桌面名称。
- 要在用户首次登录时动态创建桌面，可提供一种命名模式，并使用令牌指定顺序编号。

手动指定名称

1 为第一个池（包含从 VDIABC-01 到 VDIABC-10 的桌面名称列表）准备一个文本文件。

2 在 View Administrator 中创建池并手动指定桌面名称。

3 单击 **[Enter names（输入名称）]** 并将您的列表复制到 **[Enter Desktop Names（输入桌面名称）]** 列表框中。

4 对第二个池（使用桌面名称 VDIABC-11 到 VDIABC-20）重复这些步骤。

有关详细说明，请参阅第 92 页，“指定桌面名称列表”。

您可以在创建每个池后向其中添加桌面。例如，您可以将桌面 VDIABC-21 到 VDIABC-30 添加到第一个池中，将 VDIABC-31 到 VDIABC-40 添加到第二个池中。请参阅第 163 页，“将桌面添加到通过名称列表部署的自动池中”。

使用令牌提供命名模式

1 在 View Administrator 中创建第一个池，并使用一种命名模式部署桌面名称。

2 在命名模式文本框中键入 **VDIABC-0{n}**。

3 将池的最大大小限定为 9。

4 对第二个池重复这些步骤，但在命名模式文本框中键入 **VDIABC-1{n}**。

第一个池将包含桌面 VDIABC-01 到 VDIABC-09，第二个池将包含桌面 VDIABC-11 到 VDIABC-19。

也可以通过使用 2 位数的固定长度令牌，将每个池配置为最多包含 99 个桌面：

- 对于第一个池，键入 **VDIABC-0{n:fixed=2}**。
- 对于第二个池，键入 **VDIABC-1{n:fixed=2}**。

将每个池的最大大小限定为 99。此配置生成的桌面将具有 3 位数的顺序命名模式。

第一个池：

```
VDIABC-001
VDIABC-002
VDIABC-003
```

第二个池：

```
VDIABC-101
VDIABC-102
VDIABC-103
```

有关命名模式和令牌的详细信息，请参阅第 93 页，“为自动桌面池使用命名模式”。

手动自定义桌面

创建自动池后，您可以在不重新分配所有权的情况下自定义特定的桌面。通过在维护模式下启动桌面，您可以先修改和测试桌面，然后再将它们发布给分配的用户，或是提供给池中具有授权的所有用户使用。

- 在维护模式下自定义桌面第 95 页，

  维护模式阻止用户访问桌面。如果在维护模式下启动桌面，则创建桌面后，View Manager 会将其置于维护模式下。

- 自定义单个桌面第 95 页，

  创建池之后，您可以通过在维护模式下启动桌面来自定义各个桌面。

在维护模式下自定义桌面

维护模式阻止用户访问桌面。如果在维护模式下启动桌面，则创建桌面后，View Manager 会将其置于维护模式下。

在专用分配池中，您可以使用维护模式登录桌面，而不需要为您的管理员帐户重新分配所有权。完成自定义后，您不必将所有权返回给为桌面分配的用户。

在浮动分配池中，您可以先在维护模式下测试桌面，然后再让用户开始登录。

要对自动池中的所有桌面进行同样的自定义，可对您准备作为模板或父虚拟机的虚拟机进行自定义。View Manager 会将您的自定义操作部署到所有桌面。创建池后，您还可以使用 Sysprep 自定义规范为所有桌面配置许可、域附属、DHCP 设置以及其他计算机属性。

注意 当您为池手动指定桌面名称，而不是通过提供命名模式来命名桌面时，可以在维护模式下启动桌面。

自定义单个桌面

创建池之后，您可以通过在维护模式下启动桌面来自定义各个桌面。

步骤

1 在 View Administrator 中，启动 [Add Pool（添加池）] 向导，开始创建自动桌面池。

2 在 [Provisioning Settings（部署设置）] 页面上，选择 **[Specify names manually（手动指定名称）]**。

3 选择 **[Start desktops in maintenance mode（在维护模式下启动桌面）]**。

4 完成 [Add Pool（添加池）] 向导以完成桌面池的创建。

5 在 vCenter Server 中登录、自定义并测试各个桌面虚拟机。

  您可以手动自定义桌面，也可以使用标准的 Windows 系统管理软件（如 Altiris、SMS、LanDesk 或 BMC）来进行自定义。

6 在 View Administrator 中，选择所需的桌面池。

7 单击 **[Select all（全选）]**，或者使用过滤工具选择要发布给用户的特定桌面。

8 单击 **[More Commands（更多命令）] > [Exit Maintenance Mode（退出维护模式）]**。

下一步

通知用户他们可以登录桌面。

桌面和池的设置

在配置包含完整虚拟机的自动池、链接克隆桌面池、手动桌面池以及 Microsoft 终端服务池时，您必须指定桌面和池的设置。并非所有设置都适用于所有类型的桌面池。

表 5–19 桌面和池设置描述

设置	选项
State（状态）	■ **[Enabled（启用）]**：桌面或桌面池创建后将自动启用，并可以立即投入使用。 ■ **[Disabled（禁用）]**：桌面或桌面池创建后将被禁用，不供用户使用。如果要执行部署后的活动，如测试或其他形式的基准维护，则该设置很适用。
Connection Server restrictions（Connection Server 限制）	■ **[None（无）]**：任何 View Connection Server 实例均可以访问桌面池。 ■ **[With tags（带有标签）]**：选择一个或多个 View Connection Server 标签，可仅允许带有这些特定标签的 View Connection Server 实例访问桌面池。您可以使用复选框选择多个标签。
Remote desktop power policy（远程桌面电源策略）	确定用户从关联的桌面注销后该虚拟机的行为方式。 有关电源策略选项的描述，请参阅第 98 页，“桌面池的电源策略”。 有关电源策略对自动池的影响的更多信息，请参阅第 98 页，“为桌面池设置电源策略”。
Automatically logoff after disconnect（断开连接后自动注销）	■ **[Immediately（立即）]**：用户在断开连接后立即注销。 ■ **[Never（从不）]**：永不注销用户。 ■ **[After（之后）]**：用户断开连接的时间超过此设置后即注销。键入持续时间（以分钟为单位）。
Allow users to reset their desktops（允许用户重置桌面）	允许用户在没有管理员协助的情况下重置其桌面。
Allow multiple sessions per user（允许每个用户多个会话）	允许用户同时连接到池中的多个桌面。
Delete desktop after logoff（注销后删除桌面）	选择是否删除浮动分配的完整虚拟机桌面。 ■ **[No（否）]**：用户注销后，虚拟机保留在桌面池中。 ■ **[Yes（是）]**：用户注销后立即关闭并删除虚拟机。
Delete or refresh desktop on logoff（注销时删除或刷新桌面）	选择将浮动分配链接克隆桌面删除、刷新还是保持不变。 ■ **[Never（从不）]**：用户注销后，虚拟机保留在池中而不进行刷新。 ■ **[Delete Immediately（立即删除）]**：用户注销后立即关闭并删除虚拟机。用户注销时，View Manager 会立即将虚拟机置于 `Deleting`（正在删除）状态。 ■ **[Refresh Immediately（立即刷新）]**：用户注销后立即刷新虚拟机。用户注销时，View Manager 会立即将虚拟机置于维护模式，以防止其他用户在刷新操作开始时登录。

表 5–19 桌面和池设置描述 （续）

设置	选项
Refresh OS disk after logoff（注销后刷新操作系统磁盘）	选择是否以及何时刷新专用分配链接克隆桌面的操作系统磁盘。 ■ **[Never（从不）]**：从不刷新操作系统磁盘。 ■ **[Always（始终）]**：用户每次注销时均刷新操作系统磁盘。 ■ **[Every（间隔时间）]**：操作系统磁盘在指定的时间间隔（以天为单位）定期刷新。键入天数。 ■ **[At（特定量）]**：当操作系统磁盘当前的容量达到其允许的最大容量的指定百分比时，刷新该操作系统磁盘。链接克隆操作系统磁盘的最大容量就是副本操作系统磁盘的容量。键入启动刷新操作的百分比。 使用 **[At（特定量）]** 选项时，数据存储中的链接克隆操作系统的大小将与允许的最大容量进行对比。磁盘使用率百分比不能反映您在桌面客户操作系统中看到的磁盘使用情况。 刷新专用分配链接克隆池中的操作系统磁盘时，View Composer 永久磁盘不受影响。
Default display protocol（默认显示协议）	选择您希望 View Connection Server 与 View Client 进行通信时使用的显示协议。 **PCoIP**：受支持情况下的默认选项。PCoIP 可作为具有 Teradici 硬件的虚拟机桌面和物理机的显示协议。PCoIP 为 LAN 或 WAN 中的广大用户提供了交付的图像、音频和视频内容方面的最佳 PC 体验。 **Microsoft RDP**：Microsoft 远程桌面连接 (RDC) 使用 RDP 来传输数据。RDP 是一种允许用户远程连接计算机的多通道协议。 **HP RGS**：可作为 View Connection Server 连接 HP 刀片 PC、HP 工作站和 HP 刀片工作站时的显示协议，但不适用于虚拟机。
Allow users to choose protocol（允许用户选择协议）	允许用户使用 View Client 覆盖其桌面的默认显示协议。
Max number of monitors（显示器最大数量）	如果使用 PCoIP，您可以选择用户显示桌面时的最大显示器数量。 此设置会影响池中分配给桌面的 vRAM 量。当您将此值调大后，相关联的 ESX 主机将会消耗更多的内存。 **注意** 您必须关闭并重新启动现有的虚拟机，才能使该设置生效。重新启动虚拟机不会使设置生效。
Max resolution of any one monitor（任意一台显示器的最大分辨率）	如果使用 PCoIP，则需要选择显示器最高分辨率的像素尺寸。 此设置会影响池中分配给桌面的 vRAM 量。当您将此值调大后，相关联的 ESX 主机将会消耗更多的内存。 **注意** 您必须关闭并重新启动现有的虚拟机，才能使该设置生效。重新启动虚拟机不会使设置生效。

表 5–19 桌面和池设置描述 （续）

设置	选项
Adobe Flash quality（Adobe Flash 质量）	确定网页中显示的 Adobe Flash 内容的质量。 ■ **[Do not control（不控制）]**：质量是由网页设置确定的。 ■ **[Low（低）]**：此设置节省的带宽最多。如果未指定质量级别，系统会默认选用 [Low（低）]。 ■ **[Medium（中）]**：此设置节省的带宽适中。 ■ **[High（高）]**：此设置节省的带宽最少。 有关详细信息，请参阅第 166 页，"Adobe Flash 质量和调节"。
Adobe Flash throttling（Adobe Flash 调节）	确定 Adobe Flash 影片的帧速率。如果启用此设置，您可以通过选择激进级别减少或增加每秒显示的帧数。 ■ **[Disabled（禁用）]**：不执行调节。不修改计时器间隔。 ■ **[Conservative（保守）]**：计时器间隔为 100 毫秒。此设置可以使丢帧数达到最小。 ■ **[Moderate（中等）]**：计时器间隔为 500 毫秒。 ■ **[Aggressive（激进）]**：计时器间隔为 2500 毫秒。此设置可以使丢帧数达到最大。 有关详细信息，请参阅第 166 页，"Adobe Flash 质量和调节"。

注意 重新检入桌面前，本地桌面的属性设置不会生效。

为桌面池设置电源策略

您可以为桌面池中由 vCenter Server 管理的虚拟机配置电源策略。

电源策略可控制虚拟机在与其关联的桌面未处于使用中时的行为方式。在用户登录之前，以及用户断开连接或注销之后，桌面会被认为未处于使用中。电源策略还可以控制虚拟机在管理任务（如刷新、重构和重新平衡）完成之后的行为方式。

您可以在 View Administrator 中创建或编辑桌面池时配置电源策略。有关更多信息，请参阅第 65 页，第 5 章"创建桌面池"或第 161 页，"管理桌面池"。

注意 您无法为包含未受管的桌面的桌面池配置电源策略。

桌面池的电源策略

电源策略可控制虚拟机在其关联的 View 桌面处于未使用状态时的行为方式。

您可以在创建或编辑桌面池时设置电源策略。表 5-20 介绍了可用的电源策略。

表 5–20 电源策略

电源策略	描述
Take no power action（不执行任何电源操作）	View Manager 在用户注销后不强制执行任何电源策略。此设置有两个结果。 ■ View Manager 在用户注销后不更改虚拟机的电源状态。 例如，如果用户关闭虚拟机，则虚拟机将保持关机状态。如果用户注销而没有关机，则虚拟机将保持开机状态。当用户连接到该桌面时，虚拟机将重新启动。 ■ View Manager 在某一项管理任务完成后不强制实现任何电源状态。 例如，用户注销而没有关机，虚拟机将保持开机状态。执行计划的重构时，虚拟机将关闭。重构完成后，View Manager 不会执行任何操作来更改虚拟机的电源状态。虚拟机将保持关机状态。
Ensure desktops are always powered on（确保桌面始终开启）	虚拟机将保持开机状态，即使在未使用时也是如此。如果用户关闭虚拟机，它将立即重新启动。在刷新、重构或重新平衡等管理任务完成后，虚拟机也会重新启动。 如果您运行的批处理进程或系统管理工具必须在计划的时间与虚拟机通信，应选择 **[Ensure desktops are always powered on（确保桌面始终开启）]**。 **注意** 如果您使用 Windows Vista 系统作为链接克隆池的父虚拟机，则必须将电源策略设置为 **[Ensure desktops are always powered on（确保桌面始终开启）]**。
Suspend（挂起）	虚拟机在用户注销后进入挂起状态，但在用户断开连接时不挂起。
Power off（关机）	虚拟机在用户注销时关闭，但在用户断开连接时不关闭。

注意 当您将某个桌面添加到手动池中时，View Manager 会启动该桌面以确保其经过完整配置，即使您选择了 **[Power Off（关机）]** 或 **[Take No Power Action on Logoff（在注销时不执行任何电源操作）]** 电源策略也是如此。配置了 View Agent 后，它即会被标记为 [Ready（就绪）]，并应用池的一般电源管理设置。

对于由 vCenter Server 管理桌面的手动池，View Manager 会确保有一个备用桌面保持开启状态以供用户连接。无论应用哪种电源策略，备用桌面都会处于开启状态。

表 5–21 介绍了 View Manager 何时应用已配置的电源策略。

表 5–21 View Manager 何时应用电源策略

桌面池类型	应用的电源策略...
包含一个桌面（由 vCenter 管理的虚拟机）的手动池	电源操作由会话管理启动。虚拟机在用户请求桌面时开机，并在用户注销时关机或挂起。 **注意** 无论单一桌面池采用浮动分配还是专用分配，也无论桌面是否已分配，**[Ensure desktops are always powered on（确保桌面始终开启）]** 策略始终适用。
专用分配自动池	仅应用于未分配的桌面。 在分配的桌面中，电源操作由会话管理启动。虚拟机在用户请求已分配的桌面时开机，并在用户注销时关机或挂起。 **注意** **[Ensure desktops are always powered on（确保桌面始终开启）]** 策略适用于已分配和未分配的桌面。
浮动分配自动池	桌面未使用时，以及用户注销后。 为浮动分配桌面池配置 **[Power off（关机）]** 或 **[Suspend（挂起）]** 电源策略时，应当将 **[Automatic logoff after disconnect（断开连接后自动注销）]** 设置为 **[Immediately（立即）]**，以防止丢弃或孤立会话。

表 5–21 View Manager 何时应用电源策略 （续）

桌面池类型	应用的电源策略...
专用分配手动池	仅应用于未分配的桌面。 在分配的桌面中，电源操作由会话管理启动。虚拟机在用户请求已分配的桌面时开机，并在用户注销时关机或挂起。 **注意** **[Ensure desktops are always powered on（确保桌面始终开启）]** 策略适用于已分配和未分配的桌面。
浮动分配手动池	桌面未使用时，以及用户注销后。 为浮动分配桌面池配置 **[Power off（关机）]** 或 **[Suspend（挂起）]** 电源策略时，应当将 **[Automatic logoff after disconnect（断开连接后自动注销）]** 设置为 **[Immediately（立即）]**，以防止丢弃或孤立会话。

View Manager 将配置的电源策略应用于自动池的方式取决于桌面是否可用。有关更多信息，请参见第 100 页，“电源策略如何影响自动池”。

电源策略如何影响自动池

View 将配置的电源策略应用于自动池的方式取决于 View 桌面是否可用。

如果自动池中的桌面符合以下标准，即被认为是可用的：

- 处于活动状态
- 不包含任何用户会话
- 未分配给用户

桌面上运行的 View Agent 服务可向 View Connection Server 确认桌面的可用性。

配置自动池时，您可以指定必须部署的最大和最小虚拟机数量，以及在任意给定时间保持开机状态并且可用的备用桌面数量。

具有浮动分配的自动池电源策略示例

配置浮动分配的自动池时，可以指定在某个给定时间内可用 View 桌面的数量。无论电源策略的设置如何，可用的备用桌面始终保持开机状态。

电源策略示例 1

表 5–22 介绍了此示例中的浮动分配自动池。该池使用桌面命名模式部署及命名桌面。

表 5–22 具有浮动分配的自动桌面池设置示例 1

桌面池设置	值
Number of desktops (minimum)（最小桌面数量）	10
Number of desktops (maximum)（最大桌面数量）	20
Number of spare, powered-on desktops（备用的开机桌面数量）	2
Remote desktop power policy（远程桌面电源策略）	Suspend（挂起）

部署该桌面池时，将创建 10 个桌面，其中有两个桌面处于开机状态并随时可用，另外八个桌面处于挂起状态。

每当一个新用户连接到该池时，就会启动一个桌面，以维持可用的备用桌面数量。当连接的用户数量超过八个时，将另外创建桌面（最多创建 20 个），以维持备用桌面的数量。达到最大值后，最早断开连接的两名用户的桌面将保持开机状态，以维持备用桌面的数量。依照电源策略，每个后续用户的桌面都将挂起。

电源策略示例 2

表 5‑23 介绍了此示例中的浮动分配自动池。该池使用桌面命名模式部署及命名桌面。

表 5‑23 具有浮动分配的自动桌面池设置示例 2

桌面池设置	值
Number of desktops (minimum)（最小桌面数量）	5
Number of desktops (maximum)（最大桌面数量）	5
Number of spare, powered-on desktops（备用的开机桌面数量）	2
Remote desktop power policy（远程桌面电源策略）	Suspend（挂起）

部署该桌面池时，将创建五个桌面，其中有两个桌面处于开机状态并随时可用，另外三个桌面处于挂起状态。

如果该池中的第四个桌面被挂起，那么某个现有桌面将恢复可用。由于已经达到最大桌面数量，因此不会另外启动桌面。

具有专用分配的自动池电源策略示例

与浮动分配自动池中的已开机 View 桌面不同，专用分配自动池中不必具有可用的开机桌面。仅但桌面未分配给用户时，它才可供使用。

表 5‑24 介绍了此示例中的专用分配自动池。

表 5‑24 具有专用分配的自动桌面池设置示例

桌面池设置	值
Number of desktops (minimum)（最小桌面数量）	3
Number of desktops (maximum)（最大桌面数量）	5
Number of spare, powered-on desktops（备用的开机桌面数量）	2
Remote desktop power policy（远程桌面电源策略）	Ensure desktops are always powered on（确保桌面始终开启）

部署该桌面池时，将创建和启动三个桌面。根据电源策略，如果 vCenter Server 中关闭的桌面会立即重启。

当用户连接到池中某个桌面后，该桌面就永久分配给此用户。当用户从桌面断开连接后，该桌面将不再对其他任何用户可用。但是，**[Ensure desktops are always powered on（确保桌面始终开启）]** 策略仍然适用。如果已分配的桌面在 vCenter Server 中已关闭，那么该桌面将立即重新启动。

当另一个用户连接时，将为其分配另一个桌面。由于第二个用户连接后，备用桌面数量已降至限定数量以下，因此将创建并启动另一个桌面。每次分配一个新用户时都会创建并启动另一个桌面，直到达到最大桌面限定数量为止。

防止 View 电源策略冲突

使用 View Administrator 配置电源策略时，您必须将电源策略和客户操作系统 [Power Options（电源选项）] 控制面板中的设置进行对比，以防止发生电源策略冲突。

如果为虚拟机桌面配置的电源策略与为客户操作系统配置的电源选项不兼容，View 桌面可能会临时处于不可访问状态。如果同一池中有其他桌面，这些桌面也会受影响。

以下配置是一个电源策略冲突示例：

- 在 View Administrator 中，电源策略 **[Suspend（挂起）]** 是针对虚拟机桌面配置的。此策略将导致虚拟机在不使用时进入挂起状态。
- 在客户操作系统的 [Power Options（电源选项）] 控制面板中，**[Put the Computer to sleep（使计算机进入睡眠状态）]** 选项设置为三分钟。

在此配置中，View Connection Server 和客户操作系统都可以将虚拟机挂起。View Connection Server 期望虚拟机开机时，客户操作系统的电源选项有可能导致虚拟机不可用。

重要事项 当 Windows 7 操作系统进入睡眠模式时，其默认电源计划将导致 View 桌面临时处于不可访问状态。为阻止 Windows 7 系统进入睡眠模式，需要将电源计划设置 **[Put the computer to sleep（使计算机进入睡眠状态）]** 改为 **[Never（永不）]**。

授权用户和用户组 6

您可以配置桌面池授权，以便控制您的用户能够访问哪些 View 桌面。您也可以配置受限制的授权功能，以便根据用户在选择桌面时连接的 View Connection Server 实例来控制桌面访问。

本章讨论了以下主题：

向桌面池添加授权

在用户访问 View 桌面前，必须向他们授予使用桌面池的权限。

前提条件

创建一个桌面池。请参阅第 65 页，第 5 章“创建桌面池”。

步骤

1 在 View Administrator 中，选择 **[Inventory（清单）] > [Pools（池）]**。

2 选择桌面池并单击 **[Entitlements（授权）]**。

3 单击 **[Add（添加）]**，选择一个或多个搜索条件，然后单击 **[Find（查找）]**，以根据您设定的搜索条件查找用户或组。

注意 混合模式域搜索结果中将不包含域本地用户组。如果您的域是在混合模式下配置的，您将不能为域本地用户组中的用户授权。

4 选择要授权给池中桌面的用户或用户组，然后单击 **[OK（确定）]**。

5 单击 **[OK（确定）]** 保存更改。

移除对桌面池的授权

您可以从桌面池移除授权，以禁止特定的用户或组访问桌面。

步骤

1 在 View Administrator 中，选择 **[Inventory（清单）] > [Pools（池）]**。

2 选择桌面池并单击 **[Entitlements（授权）]**。

3 选择您要移除其授权的用户或用户组，然后单击 **[Remove（移除）]**。

4 单击 **[OK（确定）]** 保存更改。

查看桌面池授权

您可以查看某个用户或用户组有权访问的桌面池。

步骤

1 在 View Administrator 中，选择 **[Users and Groups（用户和用户组）]**，然后单击用户或用户组的名称。

2 选择 **[Summary（摘要）]** 选项卡。

   [Pool Entitlements（池授权）] 窗格会列出当前授权给用户或用户组的池。

限制 View 桌面访问

您可以配置受限制的授权功能，以根据用户在选择桌面时连接的 View Connection Server 实例限制 View 桌面访问。

使用受限制的授权功能，您可以为一个 View Connection Server 实例分配一个或多个标签。在之后配置桌面池时，您可以选择希望其能够访问桌面池的 View Connection Server 实例的标签。

当用户通过带标签的 View Connection Server 实例登录时，他们只可以访问那些没有标签或至少有一个匹配标签的桌面池。

- 受限制的授权示例第 104 页，

  此示例展示了一种包含两个 View Connection Server 实例的 View 部署。其中一个实例用于支持内部用户。另一个实例则与安全服务器配对，用于支持外部用户。

- 标签匹配第 105 页，

  受限制的授权功能通过标签匹配的方法来确定 View Connection Server 实例能否访问特定的桌面池。

- 与受限制的授权相关的考虑因素及限制因素第 106 页，

  在实施受限制的授权之前，必须注意一些考虑因素和限制因素。

- 为 View Connection Server 实例分配标签第 106 页，

  当您向 View Connection Server 实例分配标签后，与该 View Connection Server 连接的用户只能访问带有匹配标签或不带标签的 View 桌面池。

- 为桌面池分配标签第 106 页，

  当您将标签分配给桌面池后，只有连接到带有匹配标签的 View Connection Server 实例的用户才能访问该池中的桌面。

受限制的授权示例

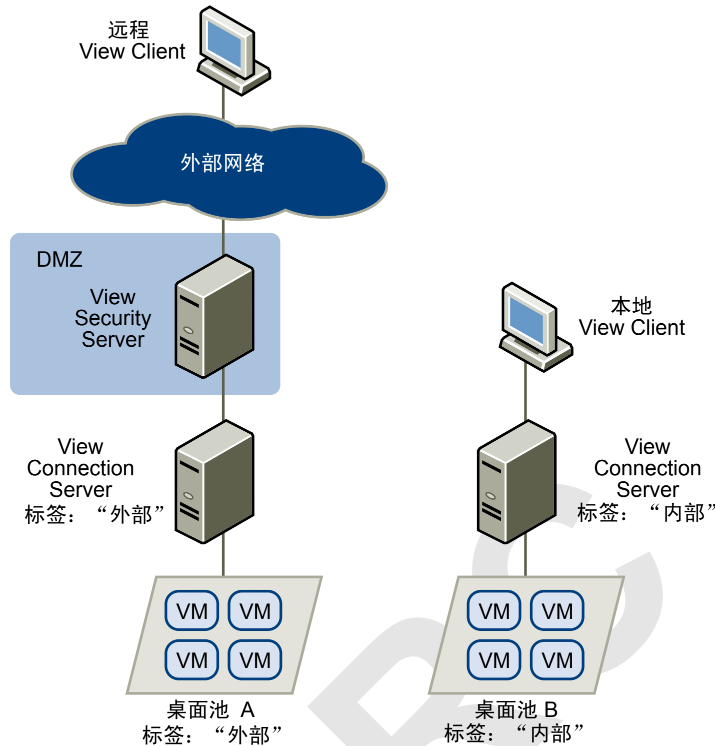
此示例展示了一种包含两个 View Connection Server 实例的 View 部署。其中一个实例用于支持内部用户。另一个实例则与安全服务器配对，用于支持外部用户。

为防止外部用户访问特定桌面，您可以采用以下操作设置受限制的授权：

- 将“内部”标签分配给支持内部用户的 View Connection Server 实例。
- 将“外部”标签分配给与安全服务器配对并支持外部用户的 View Connection Server 实例。
- 将“内部”标签分配给仅供内部用户访问的桌面池。
- 将“外部”标签分配给仅供外部用户访问的桌面池。

外部用户无法看到带有“内部”标签的桌面池，因为他们是通过带有“外部”标签的 View Connection Server 登录的；而内部用户无法看到带有“外部”标签的桌面池，因为他们是通过带有“内部”标签的 View Connection Server 登录的。图 6‑1 显示了此配置。

图 6‑1 受限制的授权配置



您也可以使用受限制的授权功能，根据您为特定 View Connection Server 实例配置的用户身份验证方法控制桌面访问。例如，您可以仅允许经过智能卡身份验证的用户使用特定的桌面池。

标签匹配

受限制的授权功能通过标签匹配的方法来确定 View Connection Server 实例能否访问特定的桌面池。

从最基本的层面来看，标签匹配方法可确定带有特定标签的 View Connection Server 实例能否访问带有相同标签的桌面池。

如果未分配标签，还会影响到 View Connection Server 实例能否访问桌面池。例如，不带有任何标签的 View Connection Server 实例只能访问同样不带任何标签的桌面池。

表 6‑1 显示了受限制的授权功能如何确定 View Connection Server 在哪些情况下能访问桌面池。

表 6‑1 标签匹配规则

View Connection Server	桌面池	是否允许访问
无标签	无标签	是
无标签	一个或多个标签	否
一个或多个标签	无标签	是
一个或多个标签	一个或多个标签	仅标签匹配时允许访问

受限制的授权功能只能强制执行标签匹配。您必须设计网络拓扑结构以强制特定的客户端通过特定的 View Connection Server 实例进行连接。

与受限制的授权相关的考虑因素及限制因素

在实施受限制的授权之前，必须注意一些考虑因素和限制因素。

- 一个 View Connection Server 实例或桌面池可以有多个标签。
- 多个 View Connection Server 实例和桌面池可以有相同的标签。
- 不带任何标签的桌面池可被任何 View Connection Server 实例访问。
- 不带任何标签的 View Connection Server 实例只能访问同样不带任何标签的桌面池。
- 如果使用安全服务器，必须在与其配对的 View Connection Server 实例上配置受限制的授权。您无法在安全服务器上配置受限制的授权。
- 如果 View Connection Server 实例的标签已被分配到桌面池，且不存在带有匹配标签的其他 View Connection Server 实例，您将无法修改或移除这些标签。
- 受限制的授权优先于其他桌面授权。例如，即使用户已获得访问某个桌面的权限，但如果这个桌面池的标签与用户连接的 View Connection Server 实例所带的标签不匹配，用户也无法访问此桌面。

为 View Connection Server 实例分配标签

当您向 View Connection Server 实例分配标签后，与该 View Connection Server 连接的用户只能访问带有匹配标签或不带标签的 View 桌面池。

步骤

1. 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Servers（服务器）]**。
2. 在 View Connection Server 中，选择所需的 View Connection Server 实例，然后单击 **[Edit（编辑）]**。
3. 在 **[Tags（标签）]** 文本框中键入一个或多个标签。

   用逗号或分号分隔多个标签。
4. 单击 **[OK（确定）]** 保存更改。

下一步

为桌面池分配标签。

为桌面池分配标签

当您将标签分配给桌面池后，只有连接到带有匹配标签的 View Connection Server 实例的用户才能访问该池中的桌面。

您可以在添加或编辑桌面池时分配标签。

前提条件

将标签分配给一个或多个 View Connection Server 实例。

步骤

1. 在 View Administrator 中，选择 **[Inventory（清单）] > [Pools（池）]**。
2. 选择您想要为其分配标签的池。

选项	操作
为新池分配标签	单击 **[Add（添加）]** 启动 [Add Pool（添加池）] 向导，然后定义并标识该池。
为已有池分配标签	选择池，然后单击 **[Edit（编辑）]**。

3 转到 [Pool Settings（池设置）] 页面。

选项	操作
新池的设置	单击 [Add Pool（添加池）] 向导中的 **[Pool Settings（池设置）]**。
已有池的设置	选择 **[Pool Settings（池 设置）]** 选项卡。

4 单击 **[Connection server restrictions（Connection Server 限制）]** 旁的 **[Browse（浏览）]**，然后配置可以访问桌面池的 View Connection Server 实例。

选项	操作
使池可供任意 View Connection Server 实例访问	选择 **[No Restrictions（无限制）]**。
使池仅供带有这些标签的 View Connection Server 实例访问	选择 **[Restrict to these tags（仅限于这些标签）]** 并选择一个或多个标签。您可以使用复选框选择多个标签。

5 单击 **[OK（确定）]** 保存更改。

设置用户身份验证 7

View 可利用您现有的 Active Directory 基础架构对用户进行身份验证和管理。为提高安全性，您可以在 View 中集成智能卡身份验证和 RSA SecurID 解决方案。

本章讨论了以下主题：

使用智能卡身份验证

您可以配置一个 View Connection Server 实例或安全服务器，以便 View 桌面用户通过智能卡进行身份验证。智能卡有时被称为通用存取卡 (Common Access Card，CAC)。

智能卡是一种内含计算机芯片的小型塑料卡。其中的芯片就像一个微型计算机，具备数据安全存储，可存储私钥和公钥证书。

使用智能卡身份验证时，用户需要将智能卡插入已连接到客户端计算机的智能卡读卡器中，并输入 PIN 码。智能卡身份验证提供了双因素身份验证功能，即检验用户是否具有智能卡以及是否知道 PIN 码。

有关实施智能卡身份验证所需的软硬件要求的信息，请参阅*《VMware View 安装指南》*。Microsoft TechNet 网站包含有关 Windows 系统中计划和实施智能卡身份验证的详细信息。

适用于 Mac 的 View Client 或 View Administrator 不支持智能卡身份验证。有关智能卡支持的完整信息，请参阅*《VMware View 体系结构规划指南》*。

使用智能卡登录

当用户将智能卡插入智能卡读卡器中后，智能卡上的用户证书将被复制到客户端系统上的本地证书存储中。本地证书存储中的证书可供客户端计算机上运行的所有应用程序（包括 View Client 应用程序）使用。

当用户与配置为使用智能卡身份验证的 View Connection Server 实例或安全服务器建立连接时，View Connection Server 实例或安全服务器将向 View Client 发送受信任的证书颁发机构 (CA) 列表。View Client 将依据可用的用户证书来检查受信任 CA 列表，选择合适的证书，然后提示用户输入智能卡 PIN 码。如果存在多个有效的用户证书，View Client 会提示用户选择其中一个证书。

View Client 会将用户证书发送给 View Connection Server 实例或安全服务器，从而通过检查证书的信任和有效期限对其进行检验。通常情况下，如果用户证书已签发并且有效，用户即可成功通过身份验证。如果配置了证书撤消检查，已撤消证书的用户将无法通过身份验证。

使用智能卡身份验证时，不支持显示协议切换。若要在使用智能卡进行身份验证后更改显示协议，用户必须注销并重新登录。

使用脱机智能卡身份验证登录本地桌面

使用脱机智能卡身份验证，用户可以在桌面未连接至 View Connection Server 的情况下用智能卡登录本地桌面。

要使用脱机智能卡身份验证，用户必须使用上次登录 View Connection Server 时所用的身份验证方法。例如，如果用户第一次用智能卡 A 登录，第二次用密码身份验证登录，最后以智能卡 B 进行登录，就必须使用智能卡 B 才能实现脱机智能卡身份验证。

使用脱机智能卡身份验证时，必须使用智能卡移除策略的最新值。智能卡移除策略可确定移除智能卡后用户是否需要重新进行身份验证才能访问桌面。智能卡移除策略是一项 View Connection Server 设置。

配置智能卡身份验证

要配置智能卡身份验证，您必须获得一个根证书并将其添加到服务器信任存储区文件，修改 View Connection Server 配置属性，并配置智能卡身份验证设置。根据您所在的具体环境，您可能需要执行附加步骤。

步骤

1 从 CA 获取根证书第 110 页，

   您必须从签发证书（位于用户提供的智能卡中）的 CA 那里获取根证书。

2 从用户证书中导出根证书第 111 页，

   如果您拥有 CA 签发的用户证书或包含 CA 签发的用户证书的智能卡，那么在根证书受系统信任的情况下，您可以导出此根证书。

3 将根证书添加到服务器信任存储区文件中第 111 页，

   您必须将所有受信任用户的根证书添加到服务器信任存储区文件中，以便 View Connection Server 实例和安全服务器对智能卡用户进行身份验证，并将它们连接到 View 桌面。

4 修改 View Connection Server 配置属性第 112 页，

   您必须修改 View Connection Server 或安全服务器主机上的 View Connection Server 配置属性，才能启用智能卡身份验证。

5 在 View Administrator 中配置智能卡设置第 113 页，

   您可以使用 View Administrator 指定设置，以适应不同的智能卡身份验证情形。

从 CA 获取根证书

您必须从签发证书（位于用户提供的智能卡中）的 CA 那里获取根证书。

如果您没有从为用户智能卡签发证书的 CA 那里获得根证书，您可从 CA 签发的用户证书或包含此类证书的智能卡中导出根证书。请参阅第 111 页，“从用户证书中导出根证书”。

步骤

1 从以下某个源中获取根证书。

   - 运行 Microsoft 证书服务的 Microsoft IIS 服务器。有关安装 Microsoft IIS、颁发证书以及在组织中分发证书的信息，请参见 Microsoft TechNet 网站。
   - 受信任 CA 签发的公用根证书。如果环境中具有智能卡基础架构，以及标准的智能卡分发和身份验证方式，就属于最常用的根证书源。

2 选择用于智能卡身份验证的证书。

   签发链会列出一系列签发机构。通常情况下，最好选择用户证书上一级的中间机构。

3 确认该机构未签发智能卡上的其他证书。

下一步

将根证书添加到服务器信任存储区文件中。请参阅第 111 页，“将根证书添加到服务器信任存储区文件中”。

从用户证书中导出根证书

如果您拥有 CA 签发的用户证书或包含 CA 签发的用户证书的智能卡，那么在根证书受系统信任的情况下，您可以导出此根证书。

步骤

1 如果用户证书存储在智能卡上，您只需将智能卡插入读卡器，就可以将用户证书添加到您的个人存储区中。

   如果用户证书未显示在您的个人存储区中，可使用读取器软件将用户证书导出到文件中。

2 在 Internet Explorer 中，选择**[Tools（工具）] > [Internet Options（Internet 选项）]**。

3 在 **[Content（内容）]** 选项卡上，单击 **[Certificates（证书）]**。

4 在 **[Personal（个人）]** 选项卡上，选择您要使用的证书，然后单击 **[View（查看）]**。

   如果用户证书未显示在列表中，请单击 **[Import（导入）]** 从文件中手动导入该证书。导入证书后，您就可以从列表中选择该证书。

5 在 **[Certification Path（证书路径）]** 选项卡上，选择树状结构顶端的证书，然后单击 **[View Certificate（查看证书）]**。

   如果用户证书是作为信任层次结构的一部分签发的，则签发证书可能由另一较高级别的证书签发。选择父证书（即实际签发用户证书的证书）作为您的根证书。

6 在 **[Details（详细信息）]** 选项卡上，单击 **[Copy to File（复制到文件）]**。

   屏幕上将显示 [Certificate Export Wizard（证书导出向导）]。

7 单击 **[Next（下一步）] > [Next（下一步）]**，为您要导出的文件键入名称和位置。

8 单击 **[Next（下一步）]** 将该文件作为根证书保存到指定的位置。

下一步

将根证书添加到服务器信任存储区文件中。

将根证书添加到服务器信任存储区文件中

您必须将所有受信任用户的根证书添加到服务器信任存储区文件中，以便 View Connection Server 实例和安全服务器对智能卡用户进行身份验证，并将它们连接到 View 桌面。

前提条件

- 从签发证书（位于用户提供的智能卡中）的 CA 那里获取根证书。请参阅第 110 页，“从 CA 获取根证书”。
- 确认 `keytool` 实用程序已添加到 View Connection Server 或安全服务器主机上的系统路径。有关更多信息，请参阅《*VMware View 安装指南*》。

步骤

1 在 View Connection Server 或安全服务器主机上，使用 `keytool` 实用程序将根证书导入服务器信任存储区文件中。

例如：**keytool -import -alias *别名* -file *根证书* -keystore *truststorefile.key***

在该命令中，***别名***是信任存储区文件中新条目的不区分大小写的唯一名称，***根证书***是您已获得或导出的根证书，***truststorefile.key***是您要添加根证书的信任存储区文件的名称。如果该文件不存在，请在当前目录中创建。

注意 `keytool` 实用程序可能会提示您为信任存储区文件创建密码。如果您以后需要向信任存储区文件中添加更多证书，就必须提供此密码。

2 将信任存储区文件复制到 View Connection Server 或安全服务器主机上的 SSL 网关配置文件夹下。

例如：*安装目录*\VMware\VMware View\Server\sslgateway\conf*truststorefile.key*

下一步

修改 View Connection Server 配置属性以启用智能卡身份验证。

修改 View Connection Server 配置属性

您必须修改 View Connection Server 或安全服务器主机上的 View Connection Server 配置属性，才能启用智能卡身份验证。

前提条件

将所有受信任用户的根证书添加到服务器信任存储区文件中。

步骤

1 在 View Connection Server 或安全服务器主机的 SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。

例如：*安装目录*\VMware\VMware View\Server\sslgateway\conf\locked.properties

2 将 `trustKeyfile`、`trustStoretype` 和 `useCertAuth` 属性添加到 `locked.properties` 文件中。

   a 将 `trustKeyfile` 属性设为您的信任存储区文件名。

   b 将 `trustStoretype` 属性设为 **JKS**。

   c 将 `useCertAuth` 属性设为 **true**，以启用证书身份验证。

3 重新启动 View Connection Server 服务或安全服务器服务，使所做的更改生效。

示例 7–1 locked.properties 文件

列出的文件指定了将所有受信任用户的根证书置于文件 `lonqa.key` 中，将信任存储区类型设为 JKS，并启用证书身份验证。

```
trustKeyfile=lonqa.key
trustStoretype=JKS
useCertAuth=true
```

下一步

如果您为 View Connection Server 实例配置了智能卡身份验证，请在 View Administrator 中配置智能卡身份验证设置。您无需为安全服务器配置智能卡身份验证设置。已配置为使用智能卡身份验证的安全服务器会始终要求用户在登录时使用智能卡和 PIN 码进行身份验证。

在 View Administrator 中配置智能卡设置

您可以使用 View Administrator 指定设置，以适应不同的智能卡身份验证情形。

这些设置不会应用于安全服务器。已配置为使用智能卡身份验证的安全服务器会始终要求用户在登录时使用智能卡和 PIN 码进行身份验证。

前提条件

- 在 View Connection Server 主机上修改 View Connection Server 配置属性。
- 确认已在 View Administrator 中选中 [Global Settings（全局设置）] 对话框中的 **[Require SSL for client connections and View Administrator（需要将 SSL 用于客户端连接和 View Administrator）]** 复选框。如果未选中该复选框，您将无法配置智能卡身份验证选项。

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 选择 View Connection Server 实例，然后单击 **[Edit（编辑）]**。

3 在 **[Authentication（身份验证）]** 选项卡上，从 **[Smart card authentication（智能卡身份验证）]** 下拉菜单中选择一个配置选项。

选项	操作
Not Allowed（不允许）	在该 View Connection Server 实例上禁用了智能卡身份验证。
Optional（可选）	用户可以使用智能卡身份验证或密码身份验证连接到该 View Connection Server 实例。如果智能卡身份验证失败，用户就必须提供密码。
Required（必需）	用户连接到该 View Connection Server 实例时必须使用智能卡身份验证。 如果必须进行智能卡身份验证，那些选中 **[Log in as current user（作为当前用户登录）]** 复选框的用户在连接至 View Connection Server 实例时将无法成功通过身份验证。这些用户登录 View 桌面时必须用智能卡和 PIN 码重新进行身份验证。 **注意** 智能卡身份验证仅可替换 Windows 密码身份验证。如果已启用 SecurID，用户就必须同时使用 SecurID 和智能卡身份验证机制进行身份验证。

4 配置智能卡移除策略。

当智能卡身份验证被设置为 **[Not Allowed（不允许）]** 时，您无法配置智能卡移除策略。

选项	操作
用户移除智能卡后断开用户与 View Connection Server 的连接	选择 **[Disconnect user sessions on smart card removal（移除智能卡时断开用户会话）]** 复选框。
在用户移除智能卡时保持与 View Connection Server 的连接，并允许用户无需重新进行身份验证即可发起新的桌面会话	取消选择 **[Disconnect user sessions on smart card removal（移除智能卡时断开用户会话）]** 复选框。

智能卡移除策略不适用于在选择了 **[Log on as current user（作为当前用户登录）]** 复选框的情况下连接 View Connection Server 实例的用户，即使他们使用智能卡来登录其客户端系统，也无法使用此策略。

5 单击 **[OK（确定）]**。

6 重新启动 View Connection Server 服务。

必须重新启动 View Connection Server 服务，对智能卡设置所做的更改才能生效。智能卡设置的变化不会对当前登录的用户造成影响。

下一步

如果需要，准备 Active Directory 以进行智能卡身份验证。请参阅第 114 页，“准备 Active Directory 以进行智能卡身份验证”。

验证智能卡身份验证配置。请参阅第 115 页，“验证智能卡身份验证配置”。

准备 Active Directory 以进行智能卡身份验证

执行智能卡身份验证时，您可能需要在 Active Directory 中执行特定的任务。

- 为智能卡用户添加 UPN 第 114 页，

  由于智能卡登录基于用户主体名称 (User Principal Name, UPN)，因此在 View 中，使用智能卡进行身份验证的用户的 Active Directory 帐户必须具有有效的 UPN。

- 将根证书添加到 Enterprise NTAuth 存储区第 115 页，

  如果您通过 CA 来颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中的 Enterprise NTAuth 存储区中。如果将 Windows 域控制器作为根 CA，则不需要执行此操作步骤。

- 将根证书添加到受信任的根证书颁发机构第 115 页，

  如果您通过 CA 来颁发智能卡登录或域控制器证书，则必须在 Active Directory 中将根证书添加到 [Trusted Root Certification Authorities（受信任的根证书颁发机构）] 组策略中。如果将 Windows 域控制器作为根 CA，则不需要执行此操作步骤。

为智能卡用户添加 UPN

由于智能卡登录基于用户主体名称 (User Principal Name, UPN)，因此在 View 中，使用智能卡进行身份验证的用户的 Active Directory 帐户必须具有有效的 UPN。

如果智能卡用户所在的域不是颁发根证书的域，则必须将用户的 UPN 设置为受信任 CA 的根证书内包含的 SAN。如果您的根证书是从智能卡用户当前所在的域中颁发的，则不需要修改用户的 UPN。

注意 即便证书是从同一个域中颁发的，您也可能需要为内置 Active Directory 帐户设置 UPN。默认情况下，内置帐户（包括管理员帐户）未设置 UPN。

前提条件

- 通过查看证书属性，获取受信任 CA 的根证书中包含的 SAN。
- 如果您的 Active Directory 服务器上没有“ADSI 编辑”实用程序，请从 Microsoft 网站下载 Windows Support Tools。

步骤

1 在 Active Directory 服务器上，启动“ADSI 编辑”实用程序。
2 在左侧窗格中，展开用户所在的域，然后双击 `CN=Users`。
3 在右侧窗格中，右键单击该用户，然后单击 **[Properties（属性）]**。
4 双击 `userPrincipalName` 属性，然后键入受信任的 CA 证书的 SAN 值。
5 单击 **[OK（确定）]** 保存属性设置。

将根证书添加到 Enterprise NTAuth 存储区

如果您通过 CA 来颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中的 Enterprise NTAuth 存储区中。如果将 Windows 域控制器作为根 CA，则不需要执行此操作步骤。

步骤

◆ 在 Active Directory 服务器上，使用 `certutil` 命令将证书发布到 Enterprise NTAuth 存储区中。

  例如：**`certutil -dspublish -f`** ***根 CA 证书的路径*** **`NTAuthCA`**

该 CA 现在是颁发此类证书的受信任颁发机构。

将根证书添加到受信任的根证书颁发机构

如果您通过 CA 来颁发智能卡登录或域控制器证书，则必须在 Active Directory 中将根证书添加到 [Trusted Root Certification Authorities（受信任的根证书颁发机构）] 组策略中。如果将 Windows 域控制器作为根 CA，则不需要执行此操作步骤。

步骤

1 在您的 Active Directory 服务器上，选择 **[Start（开始）]** > **[All Programs（所有程序）]** > **[Administrative Tools（管理工具）]** > **[Active Directory Users and Computers（Active Directory 用户和计算机）]**。
2 右键单击所需的域，然后单击 **[Properties（属性）]**。
3 在 **[Group Policy（组策略）]** 选项卡上，单击 **[Open（打开）]** 打开 [Group Policy Management（组策略管理）] 插件。
4 右键单击 **[Default Domain Policy（默认域策略）]**，然后单击 **[Edit（编辑）]**。
5 展开 **[Computer Configuration（计算机配置）]** 区域，然后打开 **[Windows Settings（Windows 设置）\Security Settings（安全设置）\Public Key（公钥）]**。
6 右键单击 **[Trusted Root Certification Authorities（受信任的根证书颁发机构）]**，然后选择 **[Import（导入）]**。
7 请按照向导中的提示导入证书，然后单击 **[OK（确定）]**。
8 关闭 [Group Policy（组策略）] 窗口。

这样，域中所有系统的受信任根存储中都将具有一个证书副本。

验证智能卡身份验证配置

当您首次设置智能卡身份验证后，或智能卡身份验证无法正常工作时，应检查您的智能卡身份验证配置。

步骤

- 确认每个客户端系统都配置了 View Client、智能卡中间件、带有有效证书的智能卡和读卡器。

  有关配置智能卡软件和硬件的信息，请参见您的智能卡供应商提供的文档。

- 在每个客户端系统上，选择 **[Start（开始）]** > **[Settings（设置）]** > **[Control Panel（控制面板）]** > **[Internet Options（Internet 选项）]** > **[Content（内容）]** > **[Certificates（证书）]** > **[Personal（个人）]**，查看证书能否用于智能卡身份验证。

  用户将智能卡插入读卡器后，Windows 会将其中的证书复制到用户计算机上，以便 View Client 使用这些证书。

- 在 View Connection Server 或安全服务器主机的 `locked.properties` 文件中，检查 `[useCertAuth]` 的属性是否被设置为 **`[true]`** 且拼写正确。

  `[locked.properties]` 文件位于以下位置：*安装目录*`\VMware\VMware View\Server\sslgateway\conf`。`useCertAuth` 属性通常会被错误地拼写为 `userCertAuth`。

- 如果您在 View Connection Server 实例上配置了智能卡身份验证，请在 View Administrator 中检查智能卡的身份验证设置。

  a 选择 **[View Configuration（View 配置）]** > **[Servers（服务器）]**，然后选择所需的 View Connection Server 实例，并单击 **[Edit（编辑）]**。

  b 在 **[Authentication（身份验证）]** 选项卡上，检查 **[Smart card authentication（智能卡身份验证）]** 是否设为 **[Optional（可选）]** 或 **[Required（必需）]**。

  必须重新启动 View Connection Server 服务，对智能卡设置所做的更改才能生效。

- 如果智能卡用户所在的域不是颁发根证书的域，请验证用户的 UPN 是否设置为受信任 CA 的根证书内包含的 SAN。

  a 通过查看证书属性，找出受信任 CA 的根证书中包含的 SAN。

  b 在您的 Active Directory 服务器上，选择 **[Start（开始）]** > **[Administrative Tools（管理工具）]** > **[Active Directory Users and Computers（Active Directory 用户和计算机）]**。

  c 右键单击 **[Users（用户）]** 文件夹中的用户，然后选择 **[Properties（属性）]**。

  UPN 出现在 **[Account（帐户）]** 选项卡的 **[User Logon Name（用户登录名）]** 文本框内。

- 如果智能卡用户使用 PCoIP 显示协议连接至 View 桌面，请确认桌面源上安装了 View Agent PCoIP 智能卡子功能。PCoIP 智能卡子功能允许用户在使用 PCoIP 显示协议时使用智能卡进行身份验证。

  注意 Windows Vista 不支持 PCoIP 智能卡子功能。

- 检查 View Connection Server 或安全服务器主机上的 *驱动器*`:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` 目录下的日志文件，查看是否存在表明已启用智能卡身份验证的消息。

使用智能卡证书撤消检查

通过配置证书撤消检查，可以阻止已撤消用户证书的用户通过智能卡进行身份验证。当用户离开组织、丢失智能卡或从一个部门调往另一个部门时，其证书通常会被撤消。

View 支持通过证书撤消列表 (CRL) 和联机证书状态协议 (Online Certificate Status Protocol, OCSP) 进行证书撤消检查。CRL 是由颁发证书的 CA 发布的已撤消证书列表。OCSP 是一种证书验证协议，用于获取 X.509 证书的撤消状态。

您可以在 View Connection Server 实例或安全服务器上配置证书撤消检查。如果 View Connection Server 实例与安全服务器配对，则您要在安全服务器上配置证书撤消检查。CA 必须能够从 View Connection Server 或安全服务器主机上访问。

您可以在同一个 View Connection Server 实例或安全服务器上配置 CRL 和 OCSP。如果您配置了两种类型的证书撤消检查，View 会首先尝试使用 OCSP 检查，如果 OCSP 检查失败，则转而进行 CRL 检查。如果 CRL 检查失败，View 将不再进行 OCSP 检查。

- 登录时进行 CRL 检查第 117 页，

  如果配置了 CRL 检查，View 会构造并读取 CRL 以确定用户证书的撤消状态。

- 登录时进行 OCSP 证书撤消检查第 117 页，

  如果您配置了 OCSP 证书撤消检查，View 会向 OCSP Responder 发送请求，以确定特定用户证书的撤消状态。View 将使用 OCSP 签发证书，以检验它从 OCSP Responder 收到的响应的真伪。

- 配置 CRL 检查第 117 页，

  如果您配置了 CRL 检查，View 将读取 CRL，以确定智能卡用户证书的撤消状态。

- 配置 OCSP 证书撤消检查第 118 页，

  如果您配置了 OCSP 证书撤消检查，View 会向 OCSP Responder 发送验证请求，以确定智能卡用户证书的撤消状态。

- 智能卡证书撤消检查属性第 118 页，

  您可以设置 `locked.properties` 文件中的值，以启用和配置智能卡证书撤消检查。

登录时进行 CRL 检查

如果配置了 CRL 检查，View 会构造并读取 CRL 以确定用户证书的撤消状态。

如果证书已撤消，并且智能卡身份验证是可选操作，则 [Enter your user name and password（输入您的用户名和密码）] 对话框将出现，而用户必须提供密码进行身份验证。如果必须进行智能卡身份验证，用户会收到错误消息，并且被禁止进行身份验证。如果 View 无法读取 CRL，也会发生同样的事件。

登录时进行 OCSP 证书撤消检查

如果您配置了 OCSP 证书撤消检查，View 会向 OCSP Responder 发送请求，以确定特定用户证书的撤消状态。View 将使用 OCSP 签发证书，以检验它从 OCSP Responder 收到的响应的真伪。

如果用户证书已撤消，并且智能卡身份验证是可选操作，则 [Enter your user name and password（输入您的用户名和密码）] 对话框将出现，而用户必须提供密码进行身份验证。如果必须进行智能卡身份验证，用户会收到错误消息，并且被禁止进行身份验证。

如果 View 没有从 OCSP Responder 收到响应或响应无效，就会重新进行 CRL 检查。

配置 CRL 检查

如果您配置了 CRL 检查，View 将读取 CRL，以确定智能卡用户证书的撤消状态。

前提条件

熟悉用于 CRL 检查的 `locked.properties` 文件属性。请参阅第 118 页，“智能卡证书撤消检查属性”。

步骤

1. 在 View Connection Server 或安全服务器主机的 SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。

   例如：*安装目录*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2. 将 `enableRevocationChecking` 和 `crlLocation` 属性添加到 `locked.properties` 文件中。

   a. 将 `enableRevocationChecking` 属性设为 **`true`**，以启用智能卡证书撤消检查。

   b. 将 `crlLocation` 属性设为 CRL 的地址。此值可以是 URL 或文件路径。

3. 重新启动 View Connection Server 服务或安全服务器服务，使所做的更改生效。

示例 7–2 locked.properties 文件

列出的文件可启用智能卡身份验证和智能卡证书撤消检查，配置 CRL 检查并为 CRL 位置指定一个 URL。

```
trustKeyfile=lonqa.key
trustStoretype=JKS
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

配置 OCSP 证书撤消检查

如果您配置了 OCSP 证书撤消检查，View 会向 OCSP Responder 发送验证请求，以确定智能卡用户证书的撤消状态。

前提条件

熟悉用于 OCSP 证书撤消检查的 `locked.properties` 文件属性。请参阅第 118 页，“智能卡证书撤消检查属性”。

步骤

1 在 View Connection Server 或安全服务器主机的 SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。

例如：*安装目录*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 将 `enableRevocationChecking`、`enableOCSP`、`ocspURL` 和 `ocspSigningCert` 属性添加到 `locked.properties` 文件中。

a 将 `enableRevocationChecking` 属性设为 **true**，以启用智能卡证书撤消检查。

b 将 `enableOCSP` 属性设为 **true**，以启用 OCSP 证书撤消检查。

c 将 `ocspURL` 属性设为 OCSP Responder 的 URL。

d 将 `ocspSigningCert` 属性设为包含 OCSP Responder 签发证书的文件的位置。

3 重新启动 View Connection Server 服务或安全服务器服务，使所做的更改生效。

示例 7–3 locked.properties 文件

列出的文件可启用智能卡身份验证和智能卡证书撤消检查，配置 CRL 与 OCSP 证书撤消检查，指定 OCSP Responder 的位置，并识别包含 OCSP 签发证书的文件。

```
trustKeyfile=lonqa.key
trustStoretype=JKS
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.lonqa.int/ocsp
```

智能卡证书撤消检查属性

您可以设置 `locked.properties` 文件中的值，以启用和配置智能卡证书撤消检查。

表 7-1 列出了证书撤消检查的 `locked.properties` 文件属性。

表 7–1 智能卡证书撤消检查属性

属性	描述
`enableRevocationChecking`	将该属性设为 **true** 可启用证书撤消检查。 如果该属性设为 **false**，则禁用证书撤消检查，并忽略其他所有证书撤消检查属性。 默认值为 **false**。
`crlLocation`	指定 CRL 的位置，可以是 URL 或文件路径。 如果您不指定 URL 或者指定的 URL 无效，在 `allowCertCRLs` 被设为 **true** 或尚未指定时，View 将使用用户证书上的 CRL 列表。 如果 View 无法访问 CRL，则 CRL 检查将会失败。

表 7–1　智能卡证书撤消检查属性（续）

属性	描述
allowCertCRLs	如果该属性设为 **true**，View 将从用户证书中提取 CRL 列表。 默认值为 **true**。
enableOCSP	将该属性设为 **true** 可启用 OCSP 证书撤消检查。 默认值为 **false**。
ocspURL	指定 OCSP Responder 的 URL。
ocspResponderCert	指定包含 OCSP Responder 签发证书的文件。View 使用该证书检验 OCSP Responder 响应的真伪。
ocspSendNonce	如果该属性设为 **true**，nonce 将会随 OCSP 请求发送，以防止重复响应。 默认值为 **false**。
ocspCRLFailover	该属性设为 **true** 时，如果 OCSP 证书撤消检查失败，View 将进行 CRL 检查。 默认值为 **true**。

使用 RSA SecurID 身份验证

您可以对 View Connection Server 实例进行配置，从而要求用户在提供 Active Directory 凭据前使用 RSA SecurID 身份验证。

由于 RSA SecurID 身份验证需要使用 RSA Authentication Manager，因此必须安装 RSA Authentication Manager 服务器并且可以从 View Connection Server 主机上直接对其进行访问。

要使用 RSA SecurID 身份验证，每个用户必须具有由 RSA Authentication Manager 注册的 SecurID 令牌。RSA SecurID 令牌是硬件或软件片段，可以按固定间隔生成身份验证代码。RSA SecurID 通过要求用户同时提供 PIN 码和身份验证代码，提供了双因素身份验证功能。身份验证代码仅对 RSA SecurID 令牌可用。

如果有多个 View Connection Server 实例，则可以在一些实例上配置 RSA SecurID 身份验证，在另一些实例上配置其他的用户身份验证方式。例如，您可以仅为那些通过 Internet 远程访问 View 桌面的用户配置 RSA SecurID 身份验证。

VMware View 通过了 RSA SecurID Ready 程序的认证，支持各种 SecurID 功能，包括新建 PIN 模式、下一个令牌代码模式、RSA Authentication Manager 以及负载平衡等。

- 使用 RSA SecurID 登录第 119 页，

  当用户连接至启用了 RSA SecurID 身份验证的 View Connection Server 实例时，View Client 中会出现 RSA SecurID 登录对话框。

- 在 View Administrator 中启用 RSA SecurID 身份验证第 120 页，

  通过在 View Administrator 中修改 View Connection Server 设置，您可以为 View Connection Server 实例启用 RSA SecurID 身份验证。

- 排除 RSA SecurID 访问被拒故障第 120 页，

  View Client 通过 RSA SecurID 身份验证进行连接时访问被拒绝。

使用 RSA SecurID 登录

当用户连接至启用了 RSA SecurID 身份验证的 View Connection Server 实例时，View Client 中会出现 RSA SecurID 登录对话框。

用户需要在 RSA SecurID 登录对话框中输入 RSA SecurID 用户名和通行码。RSA SecurID 通行码通常由 PIN 码加上令牌代码组成。

用户输入其 RSA SecurID 用户名和通行码后，如果 RSA Authentication Manager 要求输入新的 RSA SecurID PIN 码，将出现 PIN 码对话框。设置新的 PIN 码后，系统将提示用户先等待下一个令牌代码再登录。如果 RSA Authentication Manager 配置为采用系统生成的 PIN 码，将出现确认 PIN 码的对话框。

成功通过 RSA Authentication Manager 验证后，系统会提示用户输入其 Active Directory 凭据。

在 View Administrator 中启用 RSA SecurID 身份验证

通过在 View Administrator 中修改 View Connection Server 设置，您可以为 View Connection Server 实例启用 RSA SecurID 身份验证。

前提条件

- 安装和配置 RSA SecurID 软件。
- 从 RSA Authentication Manager 中导出 View Connection Server 实例的 `sdconf.rec` 文件。有关更多信息，请参见 RSA Authentication Manager 文档。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 在 View Connection Server 中，选择所需的 View Connection Server 实例，然后单击 **[Edit（编辑）]**。

3 在 **[Authentication（身份验证）]** 选项卡上，选择 **[RSA Secure ID 2-Factor Authentication（RSA SecurID 双因素身份验证）]** 下的 **[Enable（启用）]**。

4 （可选）要强制 RSA SecurID 用户名与 Active Directory 中的用户名相匹配，可选择 **[Enforce SecurID and Windows user name matching（强制匹配 SecurID 与 Windows 用户名）]**。

   如果选择此选项，用户必须使用同一 RSA SecurID 用户名进行 Active Directory 身份验证。如果不选择此选项，则可以使用不同的用户名。

5 单击 **[Upload File（上传文件）]**，键入 `sdconf.rec` 文件的地址，或单击 **[Browse（浏览）]** 搜索该文件。

6 单击 **[OK（确定）]** 保存更改。

   无需重新启动 View Connection Server 服务。系统将自动分发必要的配置文件，RSA SecurID 配置可立即生效。

排除 RSA SecurID 访问被拒故障

View Client 通过 RSA SecurID 身份验证进行连接时访问被拒绝。

问题

通过 RSA SecurID 进行验证的 View Client 连接会显示 `[Access Denied（访问被拒绝）]`，且 RSA Authentication Manager 登录监视器会显示错误 `[Node Verification Failed（验证节点失败）]`。

原因

此时需重置 RSA Agent 主机节点秘密。

解决方案

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 在 View Connection Server 中，选择所需的 View Connection Server 实例，然后单击 **[Edit（编辑）]**。

3 在 **[Authentication（身份验证）]** 选项卡上，选择 **[Clear node secret（清除节点秘密）]**。

4 单击 **[OK（确定）]** 清除节点秘密。

5 在运行 RSA Authentication Manager 的计算机上，选择**[Start（开始）] > [Programs（程序）] > [RSA Security] > [RSA Authentication Manager Host Mode（RSA Authentication Manager 主机模式）]**。

6 选择 **[Agent Host（代理主机）] > [Edit Agent Host（编辑代理主机）]**。

7 从列表中选择 **[View Connection Server]**，然后取消选中 **[Node Secret Created（已创建节点秘密）]** 复选框。

   每当您进行编辑时，将默认选中 **[Node Secret Created（已创建节点秘密）]**。

8 单击 **[OK（确定）]**。

使用作为当前用户登录功能

当 View Client 用户选择 **[Log in as current user（作为当前用户登录）]** 复选框时，用户登录客户端系统时提供的凭据将被用于 View Connection Server 实例和 View 桌面的身份验证。无需进行其他用户身份验证。

为支持此功能，用户凭据应存储在 View Connection Server 实例和客户端系统中。

- 在 View Connection Server 实例中，用户凭据经过加密并与用户名、域和可选 UPN 一同存储在用户会话中。这些凭据会在进行身份验证时添加，并在会话对象被破坏时清除。用户注销、会话超时或身份验证失败时，会话对象都会被破坏。会话对象位于易失性内存中，而不是存储在 View LDAP 或磁盘文件中。
- 在客户端系统中，用户凭据经过加密存储在 Authentication Package（View Client 的一个组件）的一个表中。用户登录时这些凭据会被添加到表中，用户注销时则会从表中移除。该表位于易失性内存中。

您可以用 View Client 组策略设置控制 **[Log in as current user（作为当前用户登录）]** 复选框的可用性以及指定其默认值。您也可以用组策略指定当用户在 View Client 中选择 **[Log in as current user（作为当前用户登录）]** 复选框时，由哪个 View Connection Server 实例来接受传送的用户身份和凭据信息。

作为当前用户登录功能存在以下要求和限制：

- 客户端登录的系统上的时间必须与 View Connection Server 主机上的时间同步。
- 如果 View Connection Server 实例中的智能卡身份验证设置为 [Required（需要）]，选择了 **[Log in as current user（作为当前用户登录）]** 复选框的智能卡用户登录 View 桌面时必须再次用智能卡和 PIN 码进行身份验证。
- 如果用户在登录时选中 **[Log in as current user（作为当前用户登录）]** 复选框，则将无法检出桌面以在本地模式下使用。
- 不得在客户端系统上修改默认的 **[Access this computer from the network（通过网络访问此计算机）]** 用户权限分配。此用户权限确定了允许哪些用户和用户组通过网络连接到计算机。有关修改此用户权限后可能会发生不兼容的信息，请参阅 Microsoft 知识库 (KB) 文章 823659。

配置策略 8

您可以配置策略来控制 View 组件、桌面池和桌面用户的行为。您需要使用 View Administrator 设置客户端会话策略，使用 Active Directory 组策略设置来控制 View 组件和特定功能的行为。

本章讨论了以下主题：

在 View Administrator 中设置策略

使用 View Administrator 配置客户端会话策略。

您可以将这些策略设置为影响特定用户、特定桌面池或所有客户端会话用户。影响特定用户和桌面池的策略称为用户级策略和桌面级策略。影响所有会话和用户的策略称为全局策略。

用户级策略将从等效的桌面池策略设置继承设置。同样，池级别策略将从等效的全局策略设置继承设置。池别级策略设置优先于等效的全局策略设置。用户级策略设置优先于等效的全局和池级别策略设置。

低级别策略设置可能比等效的高级别设置更加严格或宽松。例如，如果指定桌面可检出时间的全局策略设置为 10 分钟，而等效的池级别策略设置为 5 分钟，那么对于池中的任意用户，您都可以将等效的用户级策略设置为 30 分钟。

- 配置全局策略设置第 124 页，

  您可以配置全局策略以控制所有客户端会话用户的行为。

- 配置桌面池策略第 124 页，

  您可以配置桌面级策略以影响特定桌面池。桌面级策略设置优先于等效的全局策略设置。

- 配置桌面用户策略第 124 页，

  您可以配置用户级策略以影响特定用户。用户级策略设置始终优先于等效的全局和桌面级策略设置。

- View 策略第 125 页，

  您可以将 View 策略配置为影响所有客户端会话，或者只影响指定桌面或用户。

- 本地模式策略第 125 页，

  您可以将本地模式策略配置为影响所有客户端会话，或者也可以只影响指定桌面或用户。

配置全局策略设置

您可以配置全局策略以控制所有客户端会话用户的行为。

前提条件

请熟悉策略描述。有关信息请参见以下主题：

- 第 125 页，“View 策略”
- 第 125 页，“本地模式策略”

步骤

1 在 View Administrator 中，选择 **[Policies（策略）] > [Global Policy（全局策略）]**。

   a 要配置常规会话策略，单击 **[View Policies（View 策略）]** 窗格中的 **[Edit policies（编辑策略）]**。

   b 要配置本地会话策略，单击 **[Local Session Policies（本地会话策略）]** 窗格中的 **[Edit policies（编辑策略）]**。

2 单击 **[OK（确定）]** 保存更改。

配置桌面池策略

您可以配置桌面级策略以影响特定桌面池。桌面级策略设置优先于等效的全局策略设置。

前提条件

请熟悉策略描述。有关信息请参见以下主题：

- 第 125 页，“View 策略”
- 第 125 页，“本地模式策略”

步骤

1 在 View Administrator 中，选择 **[Inventory（清单）] > [Pools（池）]**。

2 双击所需桌面池的 ID，然后单击 **[Policies（策略）]** 选项卡。

   [Policies（策略）] 选项卡将显示当前的池策略设置。如果某个设置是从等效的全局策略继承而来，**[Desktop/Pool Policy（桌面/池策略）]** 列会显示 **[Inherit（继承）]**。

3 要为池配置常规会话策略，单击 **[View Policies（View 策略）]** 窗格中的 **[Edit policies（编辑策略）]**。

4 要为池配置本地会话策略，请单击 **[Local Mode Policies（本地模式策略）]** 窗格中的 **[Edit policies（编辑策略）]**。

5 单击 **[OK（确定）]** 保存更改。

配置桌面用户策略

您可以配置用户级策略以影响特定用户。用户级策略设置始终优先于等效的全局和桌面级策略设置。

前提条件

请熟悉策略描述。请参阅第 125 页，“View 策略”。

步骤

1 在 View Administrator 中，选择 **[Inventory（清单）] > [Pools（池）]**。

2 双击所需桌面池的 ID，然后单击 **[Policies（策略）]** 选项卡。

[Policies（策略）] 选项卡将显示当前的池策略设置。如果某个设置是从等效的全局策略继承而来，**[Desktop/Pool Policy（桌面/池策略）]** 列会显示 **[Inherit（继承）]**。

3 单击 **[User Overrides（用户覆盖）]**，然后单击 **[Add User（添加用户）]**。

4 要查找用户，请单击 **[Add（添加）]**，键入用户的名称和描述，然后单击 **[Find（查找）]**。

5 从列表中选择一个或多个用户，单击 **[OK（确定）]**，然后单击 **[Next（下一步）]**。

屏幕上将显示 [Add Individual Policy（添加单个策略）] 对话框。

6 在 **[General（常规）]** 选项卡中配置常规会话策略。

7 在 **[Local（本地）]** 选项卡中为本地模式客户端配置策略。

8 单击 **[Finish（完成）]** 保存更改。

View 策略

您可以将 View 策略配置为影响所有客户端会话，或者只影响指定桌面或用户。

表 8-1 中介绍了每个 View 策略设置。

表 8-1 View 策略

策略	描述
Multimedia redirection (MMR)（多媒体重定向 (MMR)）	确定是否为客户端系统启用 MMR。 MMR 是一种 Microsoft DirectShow 过滤器，可直接通过 TCP 套接字将多媒体数据从 View 桌面中的特定编解码器转发至客户端系统。随后，直接在播放数据的客户端系统中解码数据。 默认值为 **[Allow（允许）]**。如果客户端系统没有足够的资源来处理本地多媒体解码，请将设置更改为 **[Deny（拒绝）]**。 如果客户端系统的视频显示硬件不支持覆盖功能，MMR 将无法正常运行。
USB Access（USB 访问）	确定桌面是否可以使用 USB 设备连接客户端系统。 默认值为 **[Allow（允许）]**。如果出于安全因素阻止使用外部设备，请将设置更改为 **[Deny（拒绝）]**。
Remote mode（远程模式）	确定用户是否可以连接和使用 vCenter Server 实例上运行的桌面。如果设置为 **[Deny（拒绝）]**，用户就必须在其本地计算机上检出桌面，并仅在本地模式下运行桌面。限定用户只在本地模式下运行桌面，可减少在后端服务器上运行桌面时 CPU、内存和网络带宽需求方面的相关成本。 默认值为 **[Allow（允许）]**。
PCoIP hardware acceleration（PCoIP 硬件加速）	确定是否启用 PCoIP 显示协议的硬件加速，指定分配给 PCoIP 用户会话的加速优先级。 仅在托管桌面的物理机中装有 PCoIP 硬件加速设备时，此设置才有效。 默认值为 **[Allow（允许）]**，优先级为 **[Medium（中）]**。

本地模式策略

您可以将本地模式策略配置为影响所有客户端会话，或者也可以只影响指定桌面或用户。

表 8-2 中介绍了每种本地模式策略设置。

表 8–2 本地模式策略

策略	描述
Local Mode（本地模式）	确定用户是否可以检出桌面以在本地使用。并确定检出本地桌面时用户是否能够运行这些本地桌面。默认值为 **[Allow（允许）]**。 如果在检出桌面时将该值更改为 **[Deny（拒绝）]**，那么用户在本地模式下将无法运行该桌面，并且由于该桌面仍处于检出状态，因此无法远程使用它。
User-initiated Rollback（用户启动回滚）	确定用户是否可以放弃本地桌面，还原为远程版本。 用户启动回滚进程时，远程桌面锁定将释放，本地桌面将被丢弃。如有必要，用户可以手动移除和删除包含本地桌面数据的本地文件夹。 默认值为 **[Allow（允许）]**。
Max time without server contact（未连接服务器的最长时间）	指定本地桌面在未与 View Connection Server 建立连接进行策略更新的情况下，可以运行的天数。如果超过指定的时间限制，View Client 将向用户显示一条警告消息并挂起桌面。 默认值为 **7** 天。
Target replication frequency（目标复制频率）	指定启动两次复制之间的时间间隔（天数、小时数或分钟数）。复制操作会将在本地桌面文件中所作的全部更改复制到数据中心中相应的远程桌面或 View Composer 永久磁盘。 默认值为 **[No replication（不复制）]** 设置。如果您选择 **[At a specified interval（按指定时间间隔复制）]**，默认的复制间隔为 12 小时。 通过选择 **[No replication（不复制）]**，可以禁止计划的复制。 **[No replication（不复制）]** 策略不会禁止显式复制请求。您可以在 View Administrator 中启动复制，如果 **[User initiated replication（用户启动的复制）]** 策略设置为 **[Allow（允许）]**，那么用户可以请求复制。 如果复制花费的时间比 **[Target replication frequency（目标复制频率）]** 策略中指定的时间间隔长，那么按计划启动的复制将在前一次复制完成后开始。等待处理的复制不会取消前一次复制。 例如，**[Target replication frequency（目标复制频率）]** 策略可能设置为一天。复制可能会在星期二中午开始。如果客户端计算机断开网络连接，那么复制时间可能超过 24 小时。在星期三中午，View Client with Local Mode 会启动下一复制请求。前一次复制完成后，View Client with Local Mode 会拍摄快照并启动等待处理的复制。
User deferred replication（用户延迟的复制）	确定用户是否可以暂停活动的复制。如果您启用此策略，用户就可以延迟正在进行的复制。在延迟期限结束之前，复制不会恢复，也不会开始新的复制。 默认值为 **[Deny（拒绝）]**。当值设置为 **[Allow（允许）]** 时，延迟期限为两个小时。
Disks replicated（复制的磁盘）	确定复制了哪些桌面磁盘。此策略仅影响 View Composer 链接克隆桌面。对于完整虚拟机桌面，将复制所有磁盘。 您有以下磁盘复制选择： ■ Persistent disks（永久磁盘） ■ OS disks（操作系统磁盘） ■ OS and persistent disks（操作系统磁盘和永久磁盘） 更改此策略会在下次检出桌面后影响桌面复制操作，所作更改不会影响当前已检出的桌面。 默认值为 **[Persistent disks（永久磁盘）]**。
User initiated check in（用户启动的检入）	确定是否允许用户检入本地模式下运行的桌面。 默认值为 **[Allow（允许）]**。
User initiated replication（用户启动的复制）	确定是否允许用户从本地模式下运行的桌面启动复制。 默认值为 **[Allow（允许）]**。

使用 Active Directory 组策略

您可以使用 Microsoft Windows 组策略来优化和保护 View 桌面，控制 View 组件的行为，以及配置基于位置的打印功能。

组策略是 Microsoft Windows 操作系统的一项功能，能够在 Active Directory 环境中对计算机和远程用户进行集中管理和配置。

组策略设置包含在名为 GPO 的条目中。GPO 与 Active Directory 对象相关联。您可以将 GPO 应用于整个域内的 View 组件，以控制 View 环境的各个方面。应用后，GPO 设置将存储在指定组件的本地 Windows 注册表中。

您可以使用 Microsoft Windows 组策略对象编辑器来管理组策略设置。组策略对象编辑器是一个 Microsoft 管理控制台 (Microsoft Management Console, MMC) 插件。MMC 是 Microsoft 组策略管理控制台 (Microsoft Group Policy Management Console, GPMC) 的一部分。有关安装和使用 GPMC 的信息，请访问 Microsoft TechNet 网站。

为 View 桌面创建组织单位

您应当专门在 Active Directory 中为自己的 View 桌面创建一个组织单位 (Organizational Unit, OU)。

为防止组策略设置应用于您的桌面所在域中的其他 Windows 服务器或工作站，需要为 View 组策略创建一个 GPO，并将其链接到包含您的 View 桌面的组织单位。

有关创建组织单位和 GPO 的信息，请参阅 Microsoft TechNet 网站上的 Microsoft Active Directory 文档。

为 View 桌面启用环回处理

默认情况下，用户的策略设置来自应用于 Active Directory 中的用户对象的 GPO 集。然而，在 View 环境中，GPO 应当基于用户登录的计算机来应用于用户。

启用环回处理后，将对登录到特定计算机的所有用户应用一组一致的策略，无论他们在 Active Directory 中的位置如何。

有关启用环回处理的信息，请参阅 Microsoft Active Directory 文档。

注意 环回处理仅是在 View 中处理 GPO 的一种方法。您可能还需要实施其他方法。

使用 View 组策略管理模板文件

View 包含若干针对组件的组策略管理 (Group Policy Administrative, ADM) 模板文件。您可以将这些 ADM 模板文件中的策略设置添加到 Active Directory 中现有的或新的 GPO 中，从而优化和保护 View 桌面。

View ADM 模板文件同时包含计算机配置和用户配置组策略。

- 计算机配置策略将设置应用于所有 View 桌面的策略（无论哪个用户连接到桌面）。
- 用户配置策略将设置应用于所有用户的策略（无论他们连接到哪个 View 桌面）。用户配置策略覆盖等效的计算机配置策略。

View 在 View 桌面启动时和用户登录时应用策略。

View ADM 模板文件

View ADM 模板文件安装在您的 View Connection Server 主机上的 *安装目录*`\VMware\VMware View\Server\Extras\GroupPolicyFiles` 目录中。

表 8-3 中介绍了各个 ADM 模板文件。

表 8–3 View ADM 模板文件

模板名称	模板文件	描述
VMware View Agent 配置	`vdm_agent.adm`	包含与 View Agent 的身份验证和环境组件相关的策略设置。
VMware View Client 配置	`vdm_client.adm`	包含与 View Client 配置相关的策略设置。 从 View Connection Server 主机域外部连接的客户端不受应用于 View Client 的策略的影响。
VMware View Server 配置	`vdm_server.adm`	包含与 View Connection Server 相关的策略设置。
VMware View 公共配置	`vdm_common.adm`	包含所有 View 组件中的常见策略设置。

View Agent 配置 ADM 模板设置

View Agent 配置 ADM 模板文件 (`vdm_agent.adm`) 包含与 View Agent 的身份验证和环境组件相关的策略设置。

表 8–4 中介绍了 View Agent 配置 ADM 模板文件中的各个策略设置。该模板既包含 [Computer Configuration（计算机配置）] 设置，也包含 [User Configuration（用户配置）] 设置。[User Configuration（用户配置）] 设置优先于等效的 [Computer Configuration（计算机配置）] 设置。

表 8–4 View Agent 配置模板设置

设置	计算机	用户	属性
`AllowDirectRDP`	X		确定非 View 客户端是否可以使用 RDP 直接连接到 View 桌面。如果禁用此设置，View Agent 将只允许通过 View Client 建立的受 View 管理的连接。 默认情况下启用此设置。
`AllowSingleSignon`	X		确定是否通过单点登录 (SSO) 将用户连接到 View 桌面。启用此设置后，用户在与 View Client 连接时只需输入凭据。禁用此设置时，用户必须在进行远程连接时重新进行身份验证。 默认情况下启用此设置。
`CommandsToRunOnConnect`	X		指定在会话首次连接时运行的一组命令或命令脚本。 有关更多信息，请参阅第 129 页，"在 View 桌面中运行命令"。
`CommandsToRunOnReconnect`	X		指定在会话断开后重新连接时运行的一组命令或命令脚本。 有关更多信息，请参阅第 129 页，"在 View 桌面中运行命令"。
`Connect using DNS Name（使用 DNS 名称连接）`	X		确定 View Connection Server 在连接时是否使用 DNS 名称，而不是使用主机的 IP 地址。在使用 NAT 或防火墙的情况下，如果 View Client 或 View Connection Server 无法直接使用桌面的 IP 地址，通常会启用此设置。 默认情况下禁用此设置。
`ConnectionTicketTimeout`	X		指定 View 连接票证的有效时间（以秒为单位）。 连接 View Agent 时，View 客户端使用连接票证进行验证和单点登录。出于安全性原因，连接票证仅在有限时间内有效。当用户连接到 View 桌面时，必须在连接票证超时或会话超时之前进行身份验证。 如果未配置此设置，则使用默认超时时限 900 秒。
`CredentialFilterExceptions`	X		指定不允许加载代理 CredentialFilter 的可执行文件。文件名不得包含路径或后缀。使用分号分隔多个文件名。

表 8‑4 View Agent 配置模板设置 （续）

设置	计算机	用户	属性
Disable Time Zone Synchronization（禁用时区同步）	X	X	确定 View 桌面的时区是否与连接的客户端的时区同步。仅当 View Client 配置策略的 [Disable time zone forwarding（禁用时区转发）] 设置未被禁用时，启用此设置才会生效。 默认情况下禁用此设置。
Force MMR to use software overlay（强制 MMR 使用软件覆盖）	X		确定多媒体重定向 (MMR) 功能是否使用软件覆盖而非硬件覆盖。 MMR 使用支持覆盖的视频显示硬件以获得更好的性能。由于在多显示器系统中，硬件覆盖通常仅存在于主显示器中，因此如果将视频从主显示器拖到辅助显示器中，视频将无法显示。 启用此设置可强制 MMR 在所有显示器上使用软件覆盖。
ShowDiskActivityIcon	X		此设置在此发行版中不受支持。
Toggle Display Settings Control（切换显示设置控制）	X		确定当客户端会话采用 PCoIP 显示协议时是否禁用 **[Display（显示）]** 控制面板上的 **[Settings（设置）]** 选项卡。 默认情况下启用此设置。

在 View 桌面中运行命令

您可以用 View Agent CommandsToRunOnConnect 和 CommandsToRunOnReconnect 组策略设置在用户连接和重新连接时在 View 桌面上运行命令和命令脚本。

要运行一个命令或命令脚本，请将命令名称或脚本文件路径添加到组策略设置的命令列表中。例如：

```
date
```

```
C:\Scripts\myscript.cmd
```

要运行需要访问控制台的脚本，请添加 -C 或 -c 前缀并附带一个空格。例如：

```
-c C:\Scripts\Cli_clip.cmd
```

```
-C e:\procexp.exe
```

支持的文件类型包括 .CMD、.BAT 和 .EXE。.VBS 文件无法运行，除非此类文件由 cscript.exe 或 wscript.exe 解析。例如：

```
-C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs
```

字符串总长度（包括 -C 或 -c 选项在内）不应超过 260 个字符。

发送到 View 桌面的客户端系统信息

当用户连接或重新连接到 View 桌面时，View Client 会收集客户端系统的相关信息，然后 View Connection Server 将这些信息发送到桌面。View Agent 会将客户端计算机信息写入桌面上的系统注册表路径 HKCU\Volatile Environment。

您可以向 View Agent 的 CommandsToRunOnConnect 和 CommandsToRunOnReconnect 组策略设置中添加命令，从而在用户连接和重新连接桌面时，运行从系统注册表读取这些信息的命令或命令脚本。有关更多信息，请参阅第 129 页，“在 View 桌面中运行命令”。

表 8‑5 介绍了包含客户端系统信息的注册表项，并列出了支持这些注册表项的客户端系统类型。

表 8–5 客户端系统信息

注册表项	描述	支持的客户端系统
ViewClient_IP_Address	客户端系统的 IP 地址。	Windows Wyse Thin OS Linux
ViewClient_MAC_Address	客户端系统的 MAC 地址。	Windows Wyse Thin OS Linux
ViewClient_Machine_Name	客户端系统的计算机名。	Windows Wyse Thin OS Linux
ViewClient_Machine_Domain	客户端系统的域。	Windows Linux
ViewClient_LoggedOn_Username	在 View Client 中输入的用户名。	Windows Linux
ViewClient_LoggedOn_Domainname	在 View Client 中输入的域名。	Windows **注意** 对于 Linux 客户端，请参阅 View_Client_Machine_Domain。Linux 客户端没有给出 ViewClient_LoggedOn_Domainname 的原因是 Linux 帐户没有绑定到 Windows 域。
ViewClient_Type	客户端系统的瘦客户端名或操作系统类型。	Windows Wyse Thin OS Linux
ViewClient_Broker_DNS_Name	View Connection Server 实例的 DNS 名称。	Windows Wyse Thin OS Linux
ViewClient_Broker_URL	View Connection Server 实例的 URL。	Windows Wyse Thin OS Linux
ViewClient_Broker_Tunneled	View Connection Server 安全加密链路连接的状态，可以是 true（启用）或 false（禁用）。	Windows Wyse Thin OS Linux
ViewClient_Broker_Tunnel_URL	View Connection Server 安全加密链路连接的 URL（如果启用了安全加密链路连接）。	Windows Linux
ViewClient_Broker_Remote_IP_Address	客户端系统的远程 IP 地址。	Windows Wyse Thin OS Linux
ViewClient_TimeOffset_GMT	与 GMT 的时差，格式为 HH:MM。 使用适用于 Windows 的 View Client 时，此信息将通过专用通道传送，而无法从桌面注册表的 HKCU\Volatile Environment 路径或 View Agent 日志中获得。 要禁用此行为，请启用 View Agent 的 [Disable Time Zone Synchronization（禁用时区同步）] 组策略设置。	Windows Wyse Thin OS Linux

表 8‑5 客户端系统信息 （续）

注册表项	描述	支持的客户端系统
ViewClient_TZID	Olson 时区 ID。 使用适用于 Windows 的 View Client 时，此信息将通过专用通道传送，而无法从桌面注册表的 HKCU\Volatile Environment 路径或 View Agent 日志中获得。 要禁用此行为，请启用 View Agent 的 [Disable Time Zone Synchronization（禁用时区同步）] 组策略设置。	Windows Wyse Thin OS Linux
ViewClient_Windows_Timezone	GMT 标准时间。 使用适用于 Windows 的 View Client 时，此信息将通过专用通道传送，而无法从桌面注册表的 HKCU\Volatile Environment 路径或 View Agent 日志中获得。 要禁用此行为，请启用 View Agent 的 [Disable Time Zone Synchronization（禁用时区同步）] 组策略设置。	Windows Wyse Thin OS Linux

View Client 配置 ADM 模板设置

View Client 配置 ADM 模板文件 (vdm_client.adm) 中包含与 View Client 配置相关的策略设置。

脚本定义设置

表 8‑6 中介绍了 View Client 配置 ADM 模板文件中的脚本定义设置。该模板提供了每个脚本定义设置的计算机配置和用户配置版本。[User Configuration（用户配置）] 设置优先于等效的 [Computer Configuration（计算机配置）] 设置。

表 8‑6 View Client 配置模板：脚本定义

设置	描述
Connect all USB devices to the desktop on launch（启动时将所有 USB 设备连接到桌面）	确定桌面启动时是否将客户端系统中所有可用的 USB 设备都连接到桌面。
Connect all USB devices to the desktop when they are plugged in（插入 USB 设备时将其连接到桌面）	确定将 USB 设备插入客户端系统时是否将其都连接到桌面
DesktopLayout (requires DesktopName)（桌面布局（需要 DesktopName））	指定用户登录 View 桌面时看到的 View Client 窗口布局。布局选项包括： ■ Full Screen（全屏） ■ Multimonitor（多显示器） ■ Window - Large（窗口 — 大尺寸） ■ Window - Small（窗口 — 小尺寸） 此设置仅在设置了 [DesktopName to select （要选择的桌面名称）] 时才可用。
DesktopName to select（要选择的桌面名称）	指定 View Client 在登录过程中使用的默认桌面。
Disable 3rd-party Terminal Services plugins（禁用第三方终端服务插件）	确定 View Client 是否检查作为一般 RDP 插件安装的第三方终端服务插件。如果不配置此设置，View Client 会默认检查第三方插件。此设置不会影响 View 特定插件，如 USB 重定向。
Logon DomainName（登录域名）	指定 View Client 在登录过程中使用的 NetBIOS 域。

表 8–6 View Client 配置模板：脚本定义 （续）

设置	描述
`Logon Password`（登录密码）	指定 View Client 在登录过程中使用的密码。该密码由 Active Directory 存储在纯文本中。
`Logon UserName`（登录用户名）	指定 View Client 在登录过程中使用的用户名。
`Server URL`（服务器 URL）	指定 View Client 在登录过程中使用的 URL，例如，`http://view1.example.com`。
`Suppress error messages (when fully scripted only)`（禁止错误消息（仅当完全编写了脚本文件时））	确定在登录过程中是否隐藏 View Client 错误消息。 此设置仅适用于完全编写了登录进程脚本文件的情况，如通过策略预先填写了所有必要的登录信息时。 如果由于登录信息错误而导致登录失败，用户将不会收到通知，View Client `wswc.exe` 进程将继续在后台运行。

安全性设置

表 8–7 中介绍了 View Client 配置 ADM 模板文件中的安全性设置。安全设置包含 [Computer Configuration（计算机配置）] 设置和 [User Configuration（用户配置）] 设置。[User Configuration（用户配置）] 设置优先于等效的 [Computer Configuration（计算机配置）] 设置。

表 8–7 View Client 配置模板：安全性设置

设置	计算机	用户	描述
`Allow command line credentials`（允许命令行凭据）	X		确定是否可以通过 View Client 命令行选项提供用户凭据。启用此设置后，当用户从命令行运行 View Client 时 `smartCardPIN` 和 `password` 选项不可用。 默认情况下启用此设置。
`Brokers Trusted For Delegation`（获得委派信任的 Broker）	X		指定接受用户身份和凭据信息（在用户选中了 **[Log in as current user（作为当前用户登录）]** 复选框时传送）的 View Connection Server 实例。如果您未指定任何 View Connection Server 实例，所有 View Connection Server 实例都会接受该信息。 使用以下某种格式添加 View Connection Server 实例： ■ **`domain\system$`** ■ **`system$@domain.com`** ■ View Connection Server 服务的服务主体名称（Service Principal Name，SPN）。
`Default value of the 'Log in as current user' checkbox`（“作为当前用户登录”复选框的默认值）	X	X	指定 View Client 连接对话框上 **[Log in as current user（作为当前用户登录）]** 复选框的默认值。 这项设置优先于 View Client 安装期间指定的默认值。 如果用户通过命令行运行 View Client 并指定了 `[logInAsCurrentUser]` 选项，则该值将覆盖此设置。 如果选中了 **[Log in as current user（作为当前用户登录）]** 复选框，用户在登录客户端系统时提供的身份和凭据信息会传送到 View Connection Server 实例，最后传送到 View 桌面。如果取消选择该复选框，用户必须多次输入身份和凭据信息，才能访问 View 桌面。 默认情况下禁用此设置。

表 8–7 View Client 配置模板：安全性设置 （续）

设置	计算机	用户	描述
Display option to Log in as current user（显示“作为当前用户登录”选项））	X	X	确定 **[Log in as current user（作为当前用户登录）]** 复选框是否显示在 View Client 连接对话框上。 如果显示该复选框，用户可以选择或取消选择该复选框并覆盖其默认值。如果该复选框隐藏，用户将无法从 View Client 连接对话框中覆盖其默认值。 您可以通过 **[Default value of the ‘Log in as current user’ checkbox（“作为当前用户登录”复选框的默认值）]** 策略设置指定 [Log in as current user（作为当前用户登录）] 复选框的默认值。 默认情况下启用此设置。
Enable jump list integration（启用跳转列表集成）	X		确定在 Windows 7 及更高版本系统的任务栏上的 View Client 图标中是否显示跳转列表。使用跳转列表，用户可连接最近使用的 View Connection Server 实例和 View 桌面。 共享 View Client 时，您可能不希望用户查看最近使用的桌面名称。因此，您可以通过禁用此设置来禁用跳转列表。 默认情况下启用此设置。
Enable Single Sign-On for smart card authentication（为智能卡身份验证启用单点登录）	X		确定是否为智能卡身份验证启用单点登录。启用单点登录后，View Client 会将加密的智能卡 PIN 存储到临时内存，然后再将其提交到 View Connection Server。如果禁用单点登录，View Client 将不显示自定义 PIN 对话框。
Ignore bad SSL certificate date received from the server（忽略从服务器中收到的无效 SSL 证书日期）	X		确定是否忽略与无效的服务器证书日期关联的错误。在服务器发送过期证书时会发生这些错误。
Ignore certificate revocation problems（忽略证书撤消问题）	X		确定是否忽略与撤消的服务器证书关联的错误。当服务器发出一个已撤消的证书以及客户端无法验证证书的撤消状态时，会出现这种错误。 默认情况下禁用此设置。
Ignore incorrect SSL certificate common name (host name field)（忽略不正确的 SSL 证书公用名（主机名字段））	X		确定是否忽略与错误的服务器证书公用名关联的错误。在证书上的公用名与发送该证书的服务器主机名不匹配时会发生这些错误。
Ignore incorrect usage problems（忽略用法不正确的问题）	X		确定是否忽略与服务器证书使用不当关联的错误。如果服务器发送的证书专用于某一用途，而不是用来验证发送者的身份和对服务器通信进行加密，则会发生这些错误。
Ignore unknown certificate authority problems（忽略未知证书颁发机构问题）	X		确定是否忽略与未知的服务器证书的证书颁发机构 (CA) 关联的错误。如果服务器发送的证书是由不受信任的第三方证书颁发机构签发的，则会发生这些错误。

RDP 设置

表 8–8 中介绍了 View Client 配置 ADM 模板文件中的远程桌面协议 (Remote Desktop Protocol, RDP) 设置。所有 RDP 设置均是 [User Configuration（用户配置）] 设置。

表 8–8 View Client 配置管理模板：RDP 设置

设置	描述
Audio redirection（音频重定向）	确定是否重定向 View 桌面上播放的音频信息。可选择以下设置之一： **[Disable Audio（禁用音频）]:** 音频将被禁用。 **[Play in VM (needed for VoIP USB Support)（在虚拟机中播放（VoIP USB 支持的必备条件））]:** 音频在 View 桌面内播放。此设置需要使用共享 USB 音频设备才能在客户端中播放声音。 **[Redirect to client（重定向到客户端）]:** 音频重定向到客户端。这是默认模式。 此设置仅适用于 RDP 音频。客户端中将播放通过 MMR 重定向的音频。
Bitmap cache file size in <unit> for <number>bpp bitmaps（适用于 <数字>bpp 位图的位图缓存文件大小（以 <单位> 为单位））	指定用于特定位/像素 (bpp) 位图颜色设置的位图缓存大小（以 KB 或 MB 为单位）。 针对以下单位和 bpp 组合提供了不同的设置版本： ■ KB/8bpp ■ MB/8bpp ■ MB/16bpp ■ MB/24bpp ■ MB/32bpp
Bitmap caching（位图缓存）	确定是否将远程位图缓存在本地计算机中。
Cache persistence active（缓存永久活动）	确定是否使用永久位图缓存（处于活动状态）。永久位图缓存可以提高性能，但需要更多磁盘空间。
Color depth（颜色深度）	指定 View 桌面的颜色深度。可选择以下设置之一： ■ 8 位 ■ 15 位 ■ 16 位 ■ 24 位 ■ 32 位 对于 24 位 Windows XP 系统，您必须在 **[Computer Configuration（计算机配置）] > [Administrative Templates（管理模板）] > [Windows Components（Windows 组件）] > [Terminal Services（终端服务）]** 中启用 [Limit Maximum Color Depth（限制最大颜色深度）] 策略，并将其设置为 24 位。
Cursor shadow（光标卷影）	确定是否在 View 桌面上的光标下方显示卷影。
Desktop background（桌面背景）	确定客户端连接到 View 桌面时是否显示桌面背景。
Desktop composition（桌面拼合）	（适用于 Windows Vista 或更高版本）确定是否在 View 桌面中启用桌面拼合。 启用桌面拼合时，单个窗口不再像在先前的 Microsoft Windows 版本中那样可直接绘制到屏幕或主要显示设备中。相反，其图形将重定向到视频内存的离屏外表上，然后呈现为桌面映像，并在显示器中显示。
Enable compression（启用压缩）	确定是否压缩 RDP 数据。默认情况下启用此设置。

表 8–8 View Client 配置管理模板：RDP 设置 （续）

设置	描述
Enable Credential Security Service Provider（启用凭据安全服务提供程序）	指定 View 桌面连接是否使用网络级别身份验证（Network Level Authentication，NLA）。在 Windows Vista 中，远程桌面连接默认情况下需要使用 NLA。 如果客户操作系统需要使用 NLA 进行远程桌面连接，您必须启用该设置，否则 View Client 将无法连接到 View 桌面。 除了启用该设置，您还必须满足以下条件： ■ 客户端和客户操作系统都要支持 NLA。 ■ 启用 View Connection Server 实例的客户端直接连接。使用 NLA 时，不支持安全加密链路连接。
Enable RDP Auto-Reconnect（启用 RDP 自动重新连接）	确定 RDP 协议连接失败后 RDP 客户端组件是否尝试重新连接到 View 桌面。如果启用了 View Administrator 中的 **[Use secure tunnel connection to desktop（使用指向桌面的安全加密链路连接）]** 选项，此设置将失效。默认情况下禁用此设置。 **注意** RDP 自动重新连接只适用于运行 View Agent 4.5 版或更高版本的桌面。如果桌面装有早期版本的 View Agent，部分功能将无法正常工作。
Font smoothing（字体平滑）	（适用于 Windows Vista 或更高版本）确定是否对 View 桌面的字体应用消除锯齿效果。
Menu and window animation（菜单和窗口动画）	确定客户端连接到 View 桌面时是否对菜单和窗口启用动画效果。
Redirect clipboard（重定向剪贴板）	确定客户端连接到 View 桌面时是否重定向本地剪贴板信息。
Redirect drives（重定向驱动器）	确定客户端连接到 View 桌面时是否重定向本地磁盘驱动器。
Redirect printers（重定向打印机）	确定客户端连接到 View 桌面时是否重定向本地打印机。
Redirect serial ports（重定向串行端口）	确定客户端连接到 View 桌面时是否重定向本地 COM 端口。
Redirect smart cards（重定向智能卡）	确定客户端连接到 View 桌面时是否重定向本地智能卡。 **注意** 此设置适用于 RDP 和 PCoIP 两种连接。
Redirect supported plug-and-play devices（重定向受支持的即插即用设备）	确定客户端连接到 View 桌面时是否重定向本地即插即用设备和 POS 终端设备。此行为与 View Agent 的 USB 重定向组件所管理的重定向不同。
Shadow bitmaps（卷影位图）	确定是否显示位图卷影。此设置在全屏模式下无效。
Show contents of window while dragging（拖动时显示窗口内容）	确定用户将文件夹拖到新位置时是否显示文件夹内容。
Themes（主题）	确定客户端连接到 View 桌面时是否显示主题。
Windows key combination redirection（Windows 按键组合重定向）	确定是否应用 Windows 按键组合。

常规设置

表 8–9 中介绍了 View Client 配置 ADM 模板文件中的常规设置。常规设置包含 [Computer Configuration（计算机配置）] 设置和 [User Configuration（用户配置）] 设置。[User Configuration（用户配置）] 设置优先于等效的 [Computer Configuration（计算机配置）] 设置。

表 8–9 View Client 配置模板：常规设置

设置	计算机	用户	描述
Always on top（总在最前面）		X	确定 View Client 窗口是否总显示在最前面。启用此设置可避免 Windows 任务栏遮挡全屏模式的 View Client 窗口。默认情况下启用此设置。
Default Exit Behavior For Local Mode Desktops（本地模式桌面的默认退出行为）		X	控制在本地模式下运行的桌面的默认退出行为。默认设置为 **[Shutdown（关闭）]**，此设置将导致客户操作系统关闭。

表 8–9 View Client 配置模板：常规设置 （续）

设置	计算机	用户	描述
`Delay the start of replications when starting the View Client with Local Mode`（启动 `View Client with Local Mode` 时延迟启动复制操作）	X		指定 View Client with Local Mode 启动后延迟启动复制操作的秒数。复制操作会将在本地桌面文件中所做的全部更改复制到相应的远程桌面。 下一次按计划启动的复制将在延迟时限过后开始。复制操作将以您在 View Administrator 的本地模式策略中指定的时间间隔进行。 默认延迟时限为 900 秒（15 分钟）。
`Determines if the VMware View Client should use proxy.pac file`（确定 `VMware View Client` 是否应该使用 `proxy.pac` 文件）	X		确定 View Client 是否使用代理自动配置 (Proxy Automatic Configuration, PAC) 文件。如果启用此设置，View Client 就会使用 PAC 文件。 PAC 文件（通常称为 `proxy.pac`）可帮助 Web 浏览器和其他用户代理查找适用于特殊 URL 或站点请求的相应代理服务器。 如果在多核计算机上启用此设置，则 View Client 用来查找代理服务器信息的 WinINet 应用程序可能会崩溃。如果您的计算机上出现这种问题，请禁用此设置。 默认情况下禁用此设置。 **注意** 此设置仅应用于直接连接，而不会影响安全加密链路连接。
`Disable time zone forwarding`（禁用时区转发）	X	X	确定是否禁用 View 桌面与连接的客户端之间的时区同步。
`Don't check monitor alignment on spanning`（跨越时不检查显示器是否对齐）		X	默认情况下，如果屏幕组合在一起时不能构成精确的矩形，客户端桌面将不会跨越多个显示器。启用此设置可覆盖默认设置。默认情况下禁用此设置。
`Enable multi-media acceleration`（启用多媒体加速）		X	确定是否在客户端中启用多媒体重定向 (MMR)。 如果 View Client 视频显示硬件不支持覆盖功能，MMR 将无法正常运行。MMR 策略不适用于本地桌面会话。
`Enable the shade`（启用幕帘）		X	确定是否显示 View Client 窗口顶部的幕帘菜单栏。默认情况下启用此设置。 **注意** 默认情况下，Kiosk 模式的幕帘菜单栏是禁用的。
`Pre-login message precedes smart card PIN request`（登录前的消息在智能卡 `PIN` 请求之前发送）	X		确定登录前的消息是否在智能卡 PIN 请求之前发送。禁用此设置将使登录前的消息在智能卡 PIN 请求之后发送。
`Redirect smart card readers in Local Mode`（在本地模式中重定向智能卡读卡器）	X		确定是否将智能卡读卡器重新定向到本地桌面。与客户端系统分享读卡器。 默认情况下启用此设置。
`Tunnel proxy bypass address list`（不使用安全加密链路代理的地址列表）	X		指定一个安全加密链路地址列表。代理服务器不用于这些地址。使用分号 (;) 来分隔多个条目。
`URL for View Client online help`（`View Client` 联机帮助的 `URL`）	X		指定一个可供 View Client 检索帮助页面的备用 URL。这项设置适用于因不能访问 Internet 而无法检索远程托管的帮助系统的环境。
`Pin the shade`（固定幕帘）		X	确定是否启用 [View Client] 窗口顶部的幕帘中的大头针，且不自动隐藏菜单栏。禁用幕帘时，则此设置无效。默认情况下启用此设置。

View Server 配置 ADM 模板设置

View Server 配置 ADM 模板文件 (vdm_server.adm) 中包含与所有 View Connection Server 相关的策略设置。

表 8-10 中介绍了 View Server 配置 ADM 模板文件中的各个策略设置。该模板仅包含 [Computer Configuration（计算机配置）] 设置。

表 8–10 View Server 配置模板设置

设置	属性
Recursive Enumeration of Trusted Domains（受信任域的递归枚举）	确定是否枚举服务器所在域信任的每个域。要建立完整的信任链，系统还将枚举每个受信任域所信任的域。该进程会继续递归，直到发现所有受信任的域为止。此信息将传送到 View Connection Server，以确保客户端登录后可使用所有受信任的域。 默认情况下启用此设置。如果禁用此设置，将只枚举直接受信任的域，且不会连接到远程域控制器。 在域关系复杂的环境中（如在林中的多个域之间使用多个受信任的林结构），此过程需要几分钟才能完成。

View 公共配置 ADM 模板设置

View 公共配置 ADM 模板文件 (vdm_common.adm) 中包含所有 View 组件的共有策略设置。该模板仅包含 [Computer Configuration（计算机配置）] 设置。

日志配置设置

表 8-11 中介绍了 View 公共配置 ADM 模板文件中的日志配置策略设置。

表 8–11 View 公共配置模板：日志配置设置

设置	属性
Number of days to keep production logs（保留生产日志的天数）	指定日志文件在系统中保留的天数。如果未设置任何值，将应用默认值，日志文件将保留 7 天。
Maximum number of debug logs（最大调试日志数）	指定系统中可保留的最大调试日志文件数目。当日志文件达到最大大小时，系统将不再添加更多条目，而是创建一个新的日志文件。当先前的日志文件数量达到此值时，最早的日志文件将被删除。
Maximum debug log size in Megabytes（最大调试日志大小（以 MB 为单位））	指定调试日志可以达到的最大大小（以 MB 为单位），达到此大小后系统将关闭该日志文件，并创建一个新的日志文件。
Log Directory（日志目录）	指定日志文件目录的完整路径。如果该位置不可写，将使用默认位置。对于客户端日志文件，将额外创建一个带客户端名称的目录。

性能警报设置

表 8-12 中介绍了 View 公共配置 ADM 模板文件中的性能警报设置。

表 8–12 View 公共配置模板：性能警报设置

设置	属性
CPU and Memory Sampling Interval in Seconds（CPU 和内存采样间隔（以秒为单位））	指定 CPU 和内存轮询间隔。低采样间隔会导致高日志输出级别。
Overall CPU usage percentage to issue log info（用于发布日志信息的总体 CPU 使用率）	指定开始记录系统总体 CPU 使用率的阈值。如果有多个处理器可用，此百分比即表示综合使用率。

表 8‑12 View 公共配置模板：性能警报设置 （续）

设置	属性
Overall memory usage percentage to issue log info（用于发布日志信息的总体内存使用率）	指定开始记录提交的总体系统内存使用率的阈值。提交的系统内存是进程分配的内存，操作系统已向其提交物理内存或页面文件中的页槽。
Process CPU usage percentage to issue log info（用于发布日志信息的进程 CPU 使用率）	指定开始记录任意单个进程 CPU 使用率的阈值。
Process memory usage percentage to issue log info（用于发布日志信息的进程内存使用率）	指定开始记录任意单个进程的内存使用率的阈值。
Process to check, comma separated name list allowing wild cards and exclusion（要检查进程的逗号分隔名称列表，允许使用通配符和排除）	指定一个用逗号分隔的查询列表，这些查询对应于要检查的一个或多个进程的名称。在每个查询内，您可以使用通配符来筛选列表。 ■ 星号 (*) 可匹配零个或多个字符。 ■ 问号 (?) 则严格匹配一个字符。 ■ 在查询开头添加叹号 (!) 可将该查询生成的任何结果排除在外。 例如，以下查询将选择以 **ws** 开头的所有进程，并排除以 **sys** 结尾的所有进程： **'!*sys,ws*'**

注意 性能警报设置仅适用于 View Connection Server 和 View Agent 系统，不适用于 View Client 系统。

常规设置

表 8‑13 中介绍了 View 公共配置 ADM 模板文件中的常规设置。

表 8‑13 View 公共配置模板：常规设置

设置	属性
Disk threshold for log and events in MegaBytes（日志和事件的磁盘阈值（以 MB 为单位））	指定日志和事件的最小剩余磁盘空间阈值。如果不指定任何值，将使用默认值 200。达到指定的值后，事件记录将停止。
Enable extended logging（启用扩展日志）	确定是否将跟踪和调试事件包含在日志文件中。

设置基于位置的打印

基于位置的打印功能可将物理位置接近客户端系统的打印机映射到 View 桌面，使用户能够从 View 桌面使用本地打印机和网络打印机进行打印。

通过配置 Active Directory 组策略设置 [AutoConnect Location-based Printing for VMware View（为 VMware View 自动连接基于位置的打印）]，您可以设置基于位置的打印功能，该设置位于 Microsoft 组策略对象编辑器 **[Computer Configuration（计算机配置）]** 下的 **[Software Settings（软件设置）]** 文件夹中。

注意 [AutoConnect Location-based Printing for VMware View（为 VMware View 自动连接基于位置的打印）] 是一个针对计算机的策略。无论哪个用户连接到桌面，针对计算机的策略都会应用于所有的 View 桌面。

[AutoConnect Location-based Printing for VMware View（为 VMware View 自动连接基于位置的打印）] 中实施了一个名称转换表。您可以使用表中的每一行识别一个特定的打印机，并为该打印机定义一组转换规则。转换规则确定打印机是否被映射到 View 桌面以供某个特定客户端系统使用。

当用户连接到 View 桌面后，View 会将客户端系统与表中每个打印机所关联的转换规则进行比较。如果客户端系统符合为某个打印机设置的所有转换规则，或者某个打印机没有关联的转换规则，那么 View 会在用户会话过程中将该打印机映射到 View 桌面。

您可以根据客户端系统的 IP 地址、名称和 MAC 地址，以及用户的名称和所在的组来定义转换规则。可以为某个特定打印机指定一个转换规则或者若干转换规则的组合。

用于将打印机映射到 View 桌面的信息存储在 View 桌面的一个注册表条目中，其位置为：HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect。

1 注册基于位置的打印组策略 DLL 文件第 139 页，

   您必须注册 DLL 文件 TPVMGPoACmap.dll，才能为基于位置的打印配置组策略设置。

2 配置基于位置的打印组策略第 139 页，

   要设置基于位置的打印，您需要配置 [AutoConnect Location-based Printing for VMware View（为 VMware View 自动连接基于位置的打印）] 组策略设置。该组策略设置是一个将打印机映射到 View 桌面的名称转换表。

注册基于位置的打印组策略 DLL 文件

您必须注册 DLL 文件 TPVMGPoACmap.dll，才能为基于位置的打印配置组策略设置。

View 在您的 View Connection Server 主机上的 *安装目录*\VMware\VMware View\Server\Extras\GroupPolicyFiles\ThinPrint 目录中提供了 32 位和 64 位版本的 TPVMGPoACmap.dll 文件。

步骤

1 将适当版本的 TPVMGPoACmap.dll 文件复制到您的 Active Directory 服务器或者您用来配置组策略的域计算机中。

2 用 regsvr32 实用程序注册 TPVMGPoACmap.dll 文件。

   例如：regsvr32 "C:\TPVMGPoACmap.dll"

下一步

为基于位置的打印配置组策略设置。

配置基于位置的打印组策略

要设置基于位置的打印，您需要配置 [AutoConnect Location-based Printing for VMware View（为 VMware View 自动连接基于位置的打印）] 组策略设置。该组策略设置是一个将打印机映射到 View 桌面的名称转换表。

前提条件

- 确认您的 Active Directory 服务器上或者您用来配置组策略的域计算机上具有可用的 Microsoft MMC 和组策略对象编辑器插件。
- 在您的 Active Directory 服务器上或者您用来配置组策略的域计算机上注册 DLL 文件 TPVMGPoACmap.dll。请参阅第 139 页，“注册基于位置的打印组策略 DLL 文件”。
- 熟悉 [AutoConnect Location-based Printing for VMware View（为 VMware View 自动连接基于位置的打印）] 组策略设置的语法。请参阅第 140 页，“基于位置的打印组策略设置语法”。
- 为基于位置的组策略设置创建 GPO，并将其链接到包含您的 View 桌面的 OU。有关如何为 View 组策略创建 GPO 的示例，请参阅第 143 页，“为 View 组策略创建 GPO”。
- 由于打印作业直接从 View 桌面发送到打印机，因此请确认桌面上安装了必要的打印机驱动程序。

步骤

1 在您的 Active Directory 服务器上或者您用来配置组策略的计算机上，选择**[Start（开始）] > [All Programs（所有程序）] > [Administrative Tools（管理工具）] > [Active Directory Users and Computers（Active Directory 用户和计算机）]**。

2 右键单击包含您的 View 桌面的组织单位，然后选择 **[Properties（属性）]**。

3 在 [Group Policy（组策略）] 选项卡上，单击 **[Open（打开）]** 以打开 [Group Policy Management（组策略管理）] 插件。

4 在右侧窗格中，右键单击您为基于位置的打印组策略设置创建的 GPO，然后选择 **[Edit（编辑）]**。

   屏幕上将显示 [Group Policy Object Editor（组策略对象编辑器）] 窗口。

5 展开 **[Computer Configuration（计算机配置）]**，打开 **[Software Settings（软件设置）]** 文件夹，并选择 **[AutoConnect Location-based Printing for VMware View（为 VMware View 自动连接基于位置的打印）]**。

6 在 [Policy（策略）] 窗格中，双击 **[Configure AutoConnect Location-based Printing（配置自动连接基于位置的打印）]**。

   屏幕上将显示 [AutoConnect for VMware View Location-based Printing（为 VMware View 自动连接基于位置的打印）] 窗口。

7 选择 **[Enabled（启用）]** 以启用组策略设置。

   组策略窗口中将显示转换表标题和按钮。

   重要事项 单击 **[Disabled（禁用）]** 将删除所有表条目。作为预防措施，您可以保存配置以便将来进行导入。

8 添加您希望映射到 View 桌面的打印机，并定义其关联的转换表。

9 单击 **[OK（确定）]** 保存更改。

基于位置的打印组策略设置语法

您可以用 `[AutoConnect Location-based Printing for VMware View（为 VMware View 自动连接基于位置的打印）]` 组策略设置将打印机映射到 View 桌面。

`[AutoConnect Location-based Printing for VMware View（为 VMware View 自动连接基于位置的打印）]` 是一个名称转换表，用于标识打印机和定义关联的转换规则。表 8-14 中介绍了转换表中的语法。

表 8-14 转换表的列和值

列	描述
`IP Range（IP 范围）`	指定 IP 地址范围的转换规则。 要指定特定范围的 IP 地址，请使用以下表示法： ***ip 地址-ip 地址*** 例如： **10.112.116.0-10.112.119.255** 要指定特定子网中的所有 IP 地址，请使用以下表示法： *ip 地址/子网掩码位数* 例如： **10.112.0.0/16** 键入星号可匹配任意 IP 地址。
`Client Name（客户端名称）`	指定计算机名的转换规则。 例如：**Mary's Computer** 键入星号可匹配任意计算机名。
`Mac Address（Mac 地址）`	指定 MAC 地址的转换规则。 例如：**01:23:45:67:89:ab** 键入星号可匹配任意 MAC 地址。
`User/User Group（用户/用户组）`	指定用户名或组名的转换规则。 例如：**jdoe** 键入星号可匹配任意用户名或组名。

表 8–14 转换表的列和值 （续）

列	描述
Printer Name（打印机名称）	打印机映射到 View 桌面时的名称。 例如：**PRINTER-2-CLR** 映射的名称不必与客户端系统上的打印机名称一致。
Printer Driver（打印机驱动程序）	打印机使用的驱动程序名称。 例如：**HP Color LaserJet 4700 PS** **重要事项** 由于打印作业直接从桌面发送到打印机，因此桌面上必须安装打印机驱动程序。
IP Port/ThinPrint Port（IP 端口/ThinPrint 端口）	对于网络打印机，其 IP 地址带有 **IP_** 前缀。 例如：**IP_10.114.24.1**
D	指明打印机是否为默认打印机。

您可以使用栏标题上方显示的按钮来添加、删除和移动行，以及保存和导入表条目。每个按钮都有一个等效的键盘快捷键。将鼠标停放在每个按钮上可以看到该按钮的说明和等效的键盘快捷键。例如，要在表末尾插入一行，可单击第一个表按钮，或者按 Alt+A 键。单击最后两个按钮可导入和保存表条目。

表 8–15 显示了包含两行的转换表示例。

表 8–15 基于位置的打印组策略设置示例

IP Range（IP 范围）	Client Name（客户端名称）	Mac Address（Mac 地址）	User/ User Group（用户/用户组）	Printer Name（打印机名称）	Printer Driver（打印机驱动程序）	IP Port/ThinPrint Port（IP 端口/ ThinPrint 端口）	D
*	*	*	*	PRINTER-1-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.1	
10.112.116.140-10.112.116.145	*	*	*	PRINTER-2-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.2	X

对于任何客户端系统，第一行中指定的网络打印机都会映射到 View 桌面，因为所有的转换规则栏中都显示星号。只有当客户端系统具有 10.112.116.140 到 10.112.116.145 之间的 IP 地址时，第二行中指定的网络打印机才会映射到 View 桌面。

使用终端服务组策略

您可以使用标准的 Microsoft Windows 终端服务组策略集中控制 View 桌面的配置。

要在组策略对象编辑器中找到 [Terminal Services（终端服务）] 组策略设置，请展开 **[Computer Configuration（计算机配置）]** 或 **[User Configuration（用户配置）]** 文件夹，然后展开 **[Administrative Templates（管理模板）]**、**[Windows Components（Windows 组件）]** 和 **[Terminal Services（终端服务）]** 文件夹。

常规终端服务组策略设置

常规终端服务组策略包含若干控制登录和注销行为、远程会话以及桌面显示的设置。

表 8–16 介绍了您在管理 View 桌面时可以使用的计算机配置终端服务组策略设置。

表 8–16 常规终端服务策略设置

设置	描述
Enforce Removal of Remote Desktop Wallpaper（强制移除远程桌面墙纸）	启用此设置会在远程会话过程中强制移除墙纸，从而增强低带宽连接条件下的用户体验。
Limit maximum color depth（限制最大颜色深度）	启用此设置后，您可以指定 View 桌面会话的颜色深度。

表 8–16 常规终端服务策略设置 （续）

设置	描述
Allow users to connect remotely using Terminal Services（允许用户使用终端服务进行远程连接）	启用此设置将允许用户远程连接到目标计算机。
Remove Windows Security item from Start Menu（从 [Start（开始）] 菜单移除 [Windows Security（Windows 安全性）] 项）	如果禁用此设置，[Settings（设置）] 菜单中将显示 [Windows Security（Windows 安全性）] 项，从而确保为用户提供注销机制。
Remove Disconnect option from Shut Down dialog（从 [Shut Down（关机）] 对话框移除 [Disconnect（断开连接）] 选项）	启用此设置将从 [Shut Down Windows（关闭 Windows）] 对话框移除 [Disconnect（断开连接）] 选项，减少用户连接断开（而不是注销）的几率。

针对会话的终端服务组策略设置

针对会话的终端服务组策略设置中包含可控制断开和空闲客户端会话的相关设置。

表 8–17 介绍了您在管理 View 桌面和用户的会话相关属性时可以使用的计算机配置和用户配置终端服务组策略设置。

表 8–17 针对会话的终端服务策略设置

设置	描述
Set time limit for disconnected sessions（为断开的会话设置时间限制）	启用此设置后，您可以为断开的会话设置时间限制。达到指定的时间限制后，断开的会话将被注销。
Sets a time limit for active but idle Terminal Services sessions（为处于活动状态但空闲的终端服务会话设置时间限制）	启用此设置后，您可以为空闲的会话设置时间限制。达到指定的时间限制后，空闲的会话将被注销。

您可以将这两个设置与 View 桌面电源策略结合使用，从而创建动态解决方案，挂起或关闭断开连接的 View 桌面。View 桌面挂起或关闭后，其资源即可供其他桌面使用。

Active Directory 组策略示例

在 View 中实施 Active Directory 组策略的一种方法是：为 View 桌面创建一个组织单位，并将一个或多个 GPO 链接到该组织单位。您可以使用这些 GPO 将组策略设置应用于 View 桌面，并启用环回处理。

您可以在 Active Directory 服务器或域中的任意计算机上配置策略。本示例显示了如何直接在 Active Directory 服务器上配置策略。

注意 由于每个 View 环境都存在差异，因此您可能需要执行不同的步骤来满足您所在组织的特定需求。

步骤

1 为 View 桌面创建组织单位第 143 页，

   要将组策略应用于 View 桌面且不影响同一 Active Directory 域中的其他 Windows 计算机，您可以为 View 桌面专门创建一个组织单位。

2 为 View 组策略创建 GPO 第 143 页，

   创建 GPO 并在其中包含针对 View 组件和基于位置的打印功能的组策略，并将其链接到您的 View 桌面的组织单位。

3 将 View ADM 模板添加到 GPO 中第 144 页，

   要将 View 组件组策略设置应用于您的 View 桌面，请将其 ADM 模板文件添加到 GPO。

4 为 View 桌面启用环回处理第 145 页，

   要将通常应用于某个计算机的 [User Configuration（用户配置）] 设置应用于登录该计算机的所有用户，请启用环回处理。

为 View 桌面创建组织单位

要将组策略应用于 View 桌面且不影响同一 Active Directory 域中的其他 Windows 计算机，您可以为 View 桌面专门创建一个组织单位。

步骤

1. 在您的 Active Directory 服务器上，选择 **[Start（开始）] > [All Programs（所有程序）] > [Administrative Tools（管理工具）] > [Active Directory Users and Computers（Active Directory 用户和计算机）]**。
2. 右键单击包含您的 View 桌面的域，然后选择 **[New（新建）] > [Organizational Unit（组织单位）]**。
3. 为组织单位键入一个名称，然后单击 **[OK（确定）]**。

   新组织单位将显示在左侧窗格中。
4. 将 View 桌面添加到新的组织单位：
   a. 单击左侧窗格中的 **[Computers（计算机）]**。

      域中的所有计算机对象都将显示在右侧窗格中。
   b. 在右侧窗格中右键单击代表 View 桌面的计算机对象名称，然后选择 **[Move（移动）]**。
   c. 选择组织单位，然后单击 **[OK（确定）]**。

      当您选择组织单位时，View 桌面将显示在右侧窗格中。

下一步

为 View 组策略创建 GPO。

为 View 组策略创建 GPO

创建 GPO 并在其中包含针对 View 组件和基于位置的打印功能的组策略，并将其链接到您的 View 桌面的组织单位。

前提条件

- 为 View 桌面创建一个组织单位。
- 确认您的 Active Directory 服务器上具有可用的 Microsoft MMC 和组策略对象编辑器插件。

步骤

1. 在您的 Active Directory 服务器上，选择 **[Start（开始）] > [All Programs（所有程序）] > [Administrative Tools（管理工具）] > [Active Directory Users and Computers（Active Directory 用户和计算机）]**。
2. 右键单击包含您的 View 桌面的组织单位，然后选择 **[Properties（属性）]**。
3. 在 [Group Policy（组策略）] 选项卡上，单击 **[Open（打开）]** 以打开 [Group Policy Management（组策略管理）] 插件。
4. 右键单击所需的组织单位，然后选择 **[Create and Link a GPO Here（在此创建并链接一个 GPO）]**。

5 为 GPO 键入名称，并单击 **[OK（确定）]**。

   新 GPO 将显示在左侧窗格中该组织单位的下方。

6 （可选）将 GPO 仅应用于组织单位中的特定 View 桌面：

   a 从左侧窗格中选择所需的 GPO。

   b 选择 **[Security Filtering（安全过滤）] > [Add（添加）]**。

   c 键入 View 桌面的计算机名，并单击 **[OK（确定）]**。

      View 桌面将显示在 [Security Filtering（安全过滤）] 窗格中。GPO 中的设置将仅应用于这些 View 桌面。

下一步

将 View ADM 模板添加到组策略 GPO 中。

将 View ADM 模板添加到 GPO 中

要将 View 组件组策略设置应用于您的 View 桌面，请将其 ADM 模板文件添加到 GPO。

前提条件

- 为 View 组件组策略设置创建 GPO，并将其链接到包含您的 View 桌面的组织单位。
- 确认您的 Active Directory 服务器上具有可用的 Microsoft MMC 和组策略对象编辑器插件。

步骤

1 将 View 组件 ADM 模板文件从您的 View Connection Server 主机上的 *安装目录*`\VMware\VMware View\Server\Extras\GroupPolicyFiles` 目录复制到 Active Directory 服务器中。

2 在您的 Active Directory 服务器上，选择 **[Start（开始）] > [All Programs（所有程序）] > [Administrative Tools（管理工具）] > [Active Directory Users and Computers（Active Directory 用户和计算机）]**。

3 右键单击包含您的 View 桌面的组织单位，然后选择 **[Properties（属性）]**。

4 在 [Group Policy（组策略）] 选项卡上，单击 **[Open（打开）]** 以打开 [Group Policy Management（组策略管理）] 插件。

5 在右侧窗格中，右键单击您为组策略设置创建的 GPO，然后选择 **[Edit（编辑）]**。

   屏幕上将显示 [Group Policy Object Editor（组策略对象编辑器）] 窗口。

6 在 [Group Policy Object Editor（组策略对象编辑器）] 中，右键单击 **[Computer Configuration（计算机配置）]** 下的 **[Administrative Templates（管理模板）]**，然后选择 **[Add/Remove Templates（添加/移除模板）]**。

7 单击 **[Add（添加）]**，浏览到所需的 ADM 模板文件，然后单击 **[Open（打开）]**。

8 单击 **[Close（关闭）]** 将 ADM 模板文件中的策略设置应用于 GPO。

   模板名称将显示在左侧窗格的 **[Administrative Templates（管理模板）]** 下。

9 配置组策略设置。

下一步

为 View 桌面启用环回处理。

为 View 桌面启用环回处理

要将通常应用于某个计算机的 [User Configuration（用户配置）] 设置应用于登录该计算机的所有用户，请启用环回处理。

前提条件

- 为 View 组件组策略设置创建 GPO，并将其链接到包含您的 View 桌面的组织单位。
- 确认您的 Active Directory 服务器上具有可用的 Microsoft MMC 和组策略对象编辑器插件。

步骤

1. 在您的 Active Directory 服务器上，选择 **[Start（开始）]** > **[All Programs（所有程序）]** > **[Administrative Tools（管理工具）]** > **[Active Directory Users and Computers（Active Directory 用户和计算机）]**。
2. 右键单击包含您的 View 桌面的组织单位，然后选择 **[Properties（属性）]**。
3. 在 [Group Policy（组策略）] 选项卡上，单击 **[Open（打开）]** 以打开 [Group Policy Management（组策略管理）] 插件。
4. 在右侧窗格中，右键单击您为组策略设置创建的 GPO，然后选择 **[Edit（编辑）]**。

   屏幕上将显示 [Group Policy Object Editor（组策略对象编辑器）] 窗口。
5. 展开 **[Computer Configuration（计算机配置）]** 文件夹，然后展开 **[Administrative Templates（管理模板）]**、**[System（系统）]** 以及 **[Group Policy（组策略）]** 文件夹。
6. 在右侧窗格中，右键单击 **[User Group Policy loopback processing mode（用户组策略环回处理模式）]** 并选择 **[Properties（属性）]**。
7. 在 **[Setting（设置）]** 选项卡中选择 **[Enabled（启用）]**，然后从 **[Mode（模式）]** 下拉菜单中选择一个环回处理模式。

选项	操作
Merge（合并）	应用的用户策略设置结合了计算机 GPO 与用户 GPO 中包含的设置。如果发生冲突，则优先选用计算机 GPO。
Replace（替换）	用户策略完全由与计算机关联的 GPO 定义。任何与用户关联的 GPO 都将被忽略。

8. 单击 **[OK（确定）]** 保存更改。

管理链接克隆桌面 9

借助 View Composer，您可以更新链接克隆桌面、减少其操作系统数据的大小，并在磁盘驱动器之间重新平衡链接克隆虚拟机。您也可以管理与链接克隆关联的 View Composer 永久磁盘。

- 通过桌面刷新来降低链接克隆的大小第 147 页，

  桌面刷新操作可将每个链接克隆的操作系统磁盘还原为其原始状态和大小，降低存储成本。

- 更新链接克隆桌面第 149 页，

  您可以在父虚拟机上创建新的基础映像，然后使用重构功能将更新的映像分配到链接克隆，从而更新链接克隆桌面。

- 重新平衡链接克隆桌面第 154 页，

  桌面重新平衡操作会在可用的数据存储之间重新平均分配链接克隆桌面。

- 管理 View Composer 永久磁盘第 155 页，

  您可以从链接克隆桌面分离 View Composer 永久磁盘，分离磁盘，并将其附加到另一个链接克隆。借助此功能，您可以分开管理用户信息和链接克隆桌面。

通过桌面刷新来降低链接克隆的大小

桌面刷新操作可将每个链接克隆的操作系统磁盘还原为其原始状态和大小，降低存储成本。

如果可能，请计划在非峰值时间执行刷新操作。

有关指导原则，请参阅第 148 页，“桌面刷新操作”。

前提条件

- 决定计划何时执行刷新。默认情况下，View Composer 会立即开始执行此操作。

  您仅可以对给定的一组链接克隆在某个时间计划一次刷新操作。您可以计划多个刷新操作，前提是这些操作针对不同的链接克隆。

- 决定在操作开始时强制所有用户注销，还是等每个用户注销后再刷新该用户的桌面。

  如果强制用户注销，View Manager 将在断开之前通知用户，并允许他们关闭应用程序和注销。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 通过在左侧列中双击池 ID 来选择要刷新的池。

3 选择刷新整个池，还是刷新选定的桌面。

选项	操作
刷新池中的所有桌面	在选择的池页面中，单击 **[Settings（设置）]** 选项卡。
刷新选定的桌面	a 在选择的池页面中，单击 **[Inventory（清单）]** 选项卡。 b 选择要刷新的桌面。

4 单击 **[View Composer] > [Refresh（刷新）]**。

5 按照向导中的说明刷新链接克隆桌面。

操作系统磁盘将减小到其原始大小。

在 vCenter Server 中，您可以监视链接克隆虚拟机执行刷新操作的进度。

在 View Administrator 中，通过单击 **[Inventory（清单）] > [Pools（池）]**，选择池 ID，然后再单击 **[Tasks（任务）]** 选项卡，可监视该操作。您可以单击 **[Cancel Task（取消任务）]**、**[Pause Task（暂停任务）]** 或 **[Resume Task（恢复任务）]** 来终止任务、挂起任务或恢复挂起的任务。

桌面刷新操作

随着用户与链接克隆桌面的交互，克隆桌面的操作系统磁盘也会逐步增长。桌面刷新操作可将操作系统磁盘还原至其原始状态和大小，从而降低存储成本。

刷新操作不会影响 View Composer 永久磁盘。

链接克隆使用的存储空间少于父虚拟机，后者包含完整的操作系统数据。但是，每次在客户操作系统中写入数据时，克隆的操作系统磁盘都会增大。

当 View Composer 创建链接克隆时，它会为克隆的操作系统磁盘拍摄快照。该快照会用唯一标识标注此链接克隆虚拟机。刷新操作会把操作系统磁盘恢复到该快照。

View Composer 刷新链接克隆所需的时间仅为删除并重建该克隆所需时间的一半。

在刷新操作中请遵循以下指导原则：

- 可以按需要刷新桌面池，可以将其设置为计划事件，也可以在操作系统数据达到指定的大小时进行刷新。

  您仅可以对给定的一组链接克隆在某个时间计划一次刷新操作。如果您立即开始刷新操作，此操作将覆盖以前计划的全部任务。

  您可以计划多个刷新操作，前提是这些操作针对不同的链接克隆。

  在计划新的刷新操作之前，必须取消以前计划的全部任务。

- 您可以刷新专用分配池和浮动分配池。
- 无法刷新正在运行本地会话的桌面。
- 仅当用户从其 View 桌面断开后，才可以执行刷新操作。
- 刷新操作会保留 QuickPrep 或 Sysprep 设置的唯一计算机信息。您不需要在刷新后重新运行 Sysprep 来还原系统驱动器中安装的第三方软件的 SID 或 GUID。
- 重构链接克隆后，View Manager 会为该链接克隆的操作系统磁盘拍摄新的快照。此后的刷新操作将把操作系统数据还原到该快照，而不是还原到在最初创建该链接克隆时拍摄的快照。

注意 可通过将链接克隆的页面文件和系统临时文件重定向到临时磁盘中，以降低链接克隆的增长速度。链接克隆关闭后，View Manager 会将临时磁盘替换为 View Composer 使用链接克隆池创建的原始临时磁盘的副本。此操作会将临时磁盘压缩为其原始大小。

仅当链接克隆处于 vSphere 模式且位于 ESX/ESXi 4.0 主机上时，才支持这个一次性数据选项。

您可以在创建链接克隆池时配置此选项。

更新链接克隆桌面

您可以在父虚拟机上创建新的基础映像，然后使用重构功能将更新的映像分配到链接克隆，从而更新链接克隆桌面。

- 准备父虚拟机以重构链接克隆桌面第 149 页，

  在重构链接克隆桌面池之前，您必须更新用作该链接克隆的基础映像的父虚拟机。

- 重构链接克隆桌面第 150 页，

  桌面重构会同时更新与父虚拟机绑定的所有链接克隆桌面。

- 重构能够以本地模式运行的链接克隆桌面第 151 页，

  您可以重构能够在本地模式中运行的链接克隆桌面。但是，必须先检入桌面或将其回滚到数据中心才能执行重构操作。

- 通过桌面重构来更新链接克隆第 152 页，

  在桌面重构操作中，您可以提供操作系统修补程序，安装或更新应用程序，或者修改桌面池中所有链接克隆的桌面硬件设置。

- 更正失败的重构第 152 页，

  您可以更正失败的重构。如果您在重构链接克隆时使用的不是您想要的基础映像，那么可以采取更正措施。

- 准备 ESX 主机或群集以支持父虚拟机硬件版本 7 第 153 页，

  要使用已经升级到硬件版本 7 的父虚拟机来重构链接克隆桌面，您必须在 4.0 或更高版本的 ESX/ESXi 主机或群集上部署链接克隆池，且该池必须使用 vSphere 模式。

准备父虚拟机以重构链接克隆桌面

在重构链接克隆桌面池之前，您必须更新用作该链接克隆的基础映像的父虚拟机。

View Composer 不支持重构与父虚拟机使用不同操作系统的链接克隆。例如，您不能使用 Windows 7 或 Windows Vista 父虚拟机的快照重构 Windows XP 链接克隆。

前提条件

如果您将父虚拟机的硬件升级到版本 7，请将链接克隆池部署在 ESX/ESXi 4.0 主机或群集上。无法将池部署到混合了 ESX/ESXi 4.0 主机和 ESX/ESXi 3.5 主机的群集中。

步骤

1 在 vCenter Server 中，更新父虚拟机以便重构。

   - 在父虚拟机中安装操作系统修补程序或服务包、新应用程序、应用程序更新或执行其他更改。
   - 也可以准备另一个虚拟机，以在重构过程中选作新的父虚拟机。

2 在 vCenter Server 中，关闭更新的或新的父虚拟机。

3 在 vCenter Server 中，为父虚拟机拍摄快照。

4 如果父虚拟机硬件的版本为 7，请确保链接克隆池使用 vSphere 模式。

   a 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

   b 选择要重构的池。

   c 单击 **[Desktop (View Composer)（桌面 (View Composer)）]**。

   d 选择 **[Settings（设置）]** 选项卡，并滚动以显示 **[vCenter Server]** 面板。

   e 确认 **[Using vSphere mode（使用 vSphere 模式）]** 设置为 **[Yes（是）]**。

   如果此设置为 **[No（否）]**，则部署该池的群集包含一个或多个 ESX 3.5 主机。要从包含硬件版本 7 的基础映像部署链接克隆池，必须将群集中的所有 ESX 主机都升级到版本 4.0，或者选择另一个全部是 ESX 4.0 主机的群集。还必须将该池配置为使用 vSphere 模式。有关详细信息，请参阅第 153 页，"准备 ESX 主机或群集以支持父虚拟机硬件版本 7"。

下一步

重构链接克隆桌面池。

重构链接克隆桌面

桌面重构会同时更新与父虚拟机绑定的所有链接克隆桌面。

如果可能，请计划在非峰值时间执行重构。

前提条件

- 确认您拥有父虚拟机的快照。请参阅第 149 页，"准备父虚拟机以重构链接克隆桌面"。
- 熟悉重构指南。请参阅第 152 页，"通过桌面重构来更新链接克隆"。
- 决定计划何时执行重构操作。默认情况下，View Composer 会立即开始重构。

  您仅可以对给定的一组链接克隆在某个时间计划一次重构操作。您可以计划多个重构，前提是这些操作针对不同的链接克隆。
- 决定在重构开始时强制所有用户注销，还是等每个用户注销后再重构该用户的桌面。

  如果强制用户注销，View Manager 将在断开之前通知用户，并允许他们关闭应用程序和注销。
- 确认池部署已启用。当池部署禁用时，View Manager 在重构桌面之后会停止自定义桌面。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 通过在左侧列中双击池 ID 来选择要重构的池。

3 选择重构整个池，还是重构选定的桌面。

选项	操作
重构池中的所有桌面	在选择的池页面中，单击 **[Settings（设置）]** 选项卡。
重构选定的桌面	a 在选择的池页面中，单击 **[Inventory（清单）]** 选项卡。 b 选择要重构的桌面。

4 单击 **[View Composer] > [Recompose（重构）]**。

5 按照向导中的说明重构链接克隆桌面。

   如果从 **[Settings（设置）]** 选项卡重构整个池，可以选中 **[Change the default image for new desktops（更改新桌面的默认映像）]** 框。采用此设置时，在池中创建的新桌面将使用更新的基础映像。默认情况下，此设置已选中。

   在 [Ready to Complete（准备完成）] 页面上，您可以单击 **[Show Details（显示详细信息）]** 以显示将进行重构的链接克隆桌面。

链接克隆桌面将刷新并更新。操作系统磁盘将减小到其原始大小。

在专用分配池中，未分配的链接克隆将被删除并重新创建。这时会保持指定数量的备用桌面。

在浮动分配池中，所有链接克隆将被重构。

在 vCenter Server 中，您可以监视链接克隆虚拟机执行重构的进度。

在 View Administrator 中，通过单击 **[Inventory（清单）] > [Pools（池）]**，选择池 ID，然后再单击 **[Tasks（任务）]** 选项卡，可监视该操作。您可以单击 **[Cancel Task（取消任务）]**、**[Pause Task（暂停任务）]** 或 **[Resume Task（恢复任务）]** 来终止任务、挂起任务或恢复挂起的任务。

注意 如果在创建桌面池时使用 Sysprep 自定义规范来自定义链接克隆，则可能会为重构的虚拟机生成新的 SID。有关详细信息，请参阅第 79 页，“重构使用 Sysprep 自定义的链接克隆”。

重构能够以本地模式运行的链接克隆桌面

您可以重构能够在本地模式中运行的链接克隆桌面。但是，必须先检入桌面或将其回滚到数据中心才能执行重构操作。

前提条件

- 熟悉重构指南。请参阅第 152 页，“通过桌面重构来更新链接克隆”。
- 熟悉更新基础映像和重构链接克隆桌面的过程。请参阅第 149 页，“准备父虚拟机以重构链接克隆桌面”和第 150 页，“重构链接克隆桌面”。
- 熟悉将基础映像发布到 Transfer Server 存储库的过程。请参阅第 208 页，“在 Transfer Server 存储库中发布程序包文件”。

步骤

1 检入或回滚从基础映像创建的本地链接克隆桌面。

2 启动重构操作。

   重构操作将忽略处于本地模式的桌面。

3 将基础映像发布到 Transfer Server 存储库中。

链接克隆桌面将根据新的基础映像进行更新。

用户下一次检出链接克隆桌面时，View Transfer Server 会将更新的基础映像从 Transfer Server 存储库下载到客户端计算机。View Transfer Server 还会将链接克隆的操作系统磁盘和 View Composer 永久磁盘下载到客户端计算机上。

注意 处于本地模式的桌面在重构操作期间继续使用旧的基础映像。这些桌面不会在用户检入时重构。

通过桌面重构来更新链接克隆

在桌面重构操作中，您可以提供操作系统修补程序，安装或更新应用程序，或者修改桌面池中所有链接克隆的桌面硬件设置。

要重构链接克隆桌面，您需要在 vCenter Server 中更新父虚拟机，或者选择一个不同的虚拟机作为新的父虚拟机。接下来，为新的父虚拟机配置拍摄快照。

您可以在不影响链接克隆的情况下更改父虚拟机，因为链接克隆链接到副本虚拟机，而不是直接链接到父虚拟机。

然后，您需要选择要用作桌面池新基础映像的快照，开始重构。View Composer 会创建一个新副本，将重新配置的操作系统磁盘复制到链接克隆，然后将链接克隆绑定到新副本。

重构还会刷新链接克隆，降低其操作系统磁盘的大小。

桌面重构不会影响 View Composer 永久磁盘。

在重构时请遵循以下指导原则：

- 您可以重构专用分配池和浮动分配池。
- 可以按需重构桌面池，也可以将其设置为计划事件。

  您仅可以对给定的一组链接克隆在某个时间计划一次重构操作。在计划新的重构操作之前，必须取消以前计划的全部任务或等到前一次操作完成之后。在立即启动新的重构操作之前，必须取消以前计划的全部任务。

  您可以计划多个重构，前提是这些操作针对不同的链接克隆。
- 可以重构选定的链接克隆，也可以重构桌面池中的所有链接克隆。
- 当池中的不同链接克隆派生自同一基础映像的不同快照或不同基础映像时，池中包含多个副本。
- 无法重构以本地模式运行的桌面。必须先检入本地桌面或将其回滚到数据中心，才能执行重构操作。
- 仅当用户注销其 View 桌面后，才能执行重构操作。
- 当链接克隆和新的或更新的父虚拟机使用不同的操作系统时，您无法重构链接克隆。
- 当 Windows 7 链接克隆和新的或更新的父虚拟机使用不同的操作系统磁盘控制器时，您无法重构链接克隆。

注意 如果在创建桌面池时使用 Sysprep 自定义规范来自定义链接克隆，则可能会为重构的虚拟机生成新的 SID。有关详细信息，请参阅第 79 页，“重构使用 Sysprep 自定义的链接克隆”。

更正失败的重构

您可以更正失败的重构。如果您在重构链接克隆时使用的不是您想要的基础映像，那么可以采取更正措施。

问题

重构失败时，桌面会处于错误或过期状态。

原因

在重构期间，vCenter Server 主机、vCenter Server 或数据存储中可能发生系统故障或问题。

或者，重构操作所用的虚拟机快照中所捕获的操作系统可能与原始父虚拟机的操作系统不同。例如，您可能会使用一个 Windows 7 快照重构 Windows XP 链接克隆。

解决方案

1 选择上一次成功重构时使用的快照。

您也可以选择新的快照，将链接克隆更新到新状态。

快照中所捕获的操作系统必须与原始父虚拟机快照中的操作系统相同。

2 再次重构该池。

View Composer 将从快照创建基础映像，并重新创建链接克隆操作系统磁盘。

重构期间将保留包含用户数据和设置的 View Composer 永久磁盘。

根据错误重构的情况，您可能需要刷新或重新平衡链接克隆而不是再次重构，也可能需要再次执行重构，并刷新或重新平衡链接克隆。

注意 如果您未配置 View Composer 永久磁盘，所有重构操作都会删除用户在链接克隆桌面中生成的更改。

准备 ESX 主机或群集以支持父虚拟机硬件版本 7

要使用已经升级到硬件版本 7 的父虚拟机来重构链接克隆桌面，您必须在 4.0 或更高版本的 ESX/ESXi 主机或群集上部署链接克隆池，且该池必须使用 vSphere 模式。

重构未采用 vSphere 模式的链接克隆池时，无法使用已经升级到硬件版本 7 的父虚拟机的快照。重构向导中不会显示快照。

重构链接克隆之前，请按照以下描述的过程执行操作。

前提条件

- 确认您想用来重构链接克隆的父虚拟机已升级至硬件版本 7。装有硬件版本 7 的虚拟机必须在 4.0 版或更高版本的 ESX/ESXi 主机上运行。有关升级 View 组件的更多信息，请参阅《*VMware View 升级指南*》。
- 准备父虚拟机以进行重构操作。有关详细信息，请参阅第 149 页，“准备父虚拟机以重构链接克隆桌面”。

步骤

1 在部署池的 vCenter Server 群集中，将所有 ESX 主机升级到 4.0 或更高版本。

您也可以使用另一个群集，只要该群集中的所有 ESX 主机都是 4.0 或更高版本。

2 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

3 选择要重构的池。

4 单击 **[Desktop (View Composer)（桌面 (View Composer)）]**。

5 选择 **[Settings（设置）]** 选项卡，单击 **[Edit（编辑）]**。

6 选择 **[vCenter Settings（vCenter 设置）]** 选项卡。

7 在 **[Host or Cluster（主机或群集）]** 旁边，单击 **[Select（选择）]**。

如果父虚拟机采用了硬件版本 7，则只会显示 4.0 或更高版本的 ESX 主机或群集。

8 选择一个主机或群集。

9 选中 **[Use vSphere mode for View Composer（为 View Composer 应用 vSphere 模式）]**，并单击 **[OK（确定）]**。

下一步

重构链接克隆桌面池。

重新平衡链接克隆桌面

桌面重新平衡操作会在可用的数据存储之间重新平均分配链接克隆桌面。

如果可能，请计划在非峰值时间执行重新平衡操作。

有关指导原则，请参阅第 154 页，“在逻辑驱动器之间重新平衡链接克隆”。

前提条件

- 熟悉重新平衡操作。请参阅第 154 页，“在逻辑驱动器之间重新平衡链接克隆”。
- 决定计划何时执行重新平衡操作。默认情况下，View Composer 会立即开始执行此操作。

  您仅可以对给定的一组链接克隆在某个时间计划一次重新平衡操作。您可以计划多个重新平衡操作，前提是这些操作针对不同的链接克隆。
- 决定在操作开始时强制所有用户注销，还是等每个用户注销后再重新平衡该用户的桌面。

  如果强制用户注销，View Manager 将在断开之前通知用户，并允许他们关闭应用程序和注销。
- 确认池部署已启用。当池部署禁用时，View Manager 在重新平衡桌面之后会停止自定义桌面。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 通过在左侧列中双击池 ID 来选择要重新平衡的池。

3 选择重新平衡整个池，还是重新平衡选定的桌面。

选项	操作
重新平衡池中的所有桌面	在选择的池页面中，单击 **[Settings（设置）]** 选项卡。
重新平衡选定的桌面	a 在选择的池页面中，单击 **[Inventory（清单）]** 选项卡。 b 选择要重新平衡的桌面。

4 单击 **[View Composer] > [Rebalance（重新平衡）]**。

5 按照向导中的说明重新平衡链接克隆桌面。

链接克隆桌面将刷新和重新平衡。操作系统磁盘将减小到其原始大小。

在 View Administrator 中，通过单击 **[Inventory（清单）] > [Pools（池）]**，选择池 ID，然后再单击 **[Tasks（任务）]** 选项卡，可监视该操作。您可以单击 **[Cancel Task（取消任务）]**、**[Pause Task（暂停任务）]** 或 **[Resume Task（恢复任务）]** 来终止任务、挂起任务或恢复挂起的任务。

在逻辑驱动器之间重新平衡链接克隆

重新平衡桌面操作会在可用的逻辑驱动器之间重新平均分配链接克隆桌面。它可以节省过载驱动器上的存储空间，并确保充分利用所有驱动器。

当您创建大型链接克隆桌面池并使用多个逻辑单元号 (LUN) 时，如果初始大小不准确，可能无法有效利用空间。如果设置激进的存储过载级别，链接克隆可能会快速增长，并用完数据存储中的所有可用空间。

当虚拟机使用的空间达到数据存储空间的 95% 时，View Manager 会生成一个警告日志条目。在使用的空间达到 99% 时，vSphere 会挂起数据存储中的每个虚拟机。

重新平衡还会刷新链接克隆，从而降低其操作系统磁盘的大小。这不会影响 View Composer 永久磁盘。

重新平衡桌面时请遵循以下指导原则：

- 您可以重新平衡专用分配池和浮动分配池。
- 可以重新平衡选定的链接克隆或池中的所有克隆。
- 可以按需重新平衡桌面池，也可以将其设置为计划事件。

  您仅可以对给定的一组链接克隆在某个时间计划一次重新平衡操作。如果立即开始重新平衡操作，此操作将覆盖以前计划的所有任务。

  您可以计划多个重新平衡操作，前提是这些操作针对不同的链接克隆。

  在计划新的重新平衡操作之前，必须取消之前计划的全部任务。

- 您只能重新平衡处于 [Available（可用）]、[Error（错误）] 或 [Customizing（正在自定义）] 状态且没有计划取消或等待取消的桌面。
- 最佳实践是不要将链接克隆虚拟机和其他类型的虚拟机混合存储在同一数据存储中。这样，View Composer 就可以重新平衡数据存储中的所有虚拟机。
- 如果您编辑某个池并更改主机或群集以及存储链接克隆的数据存储，则您只能在新选择的主机或群集能够完全访问原始和新数据存储的情况下，才可以重新平衡链接克隆。新群集中的所有主机必须能够访问原始和新数据存储。

  例如，您可能会在一个独立的主机上创建一个链接克隆池，并选择一个本地数据存储来存储克隆。如果您编辑该池并选择一个群集和共享数据存储，重新平衡操作将会因为群集中的主机无法访问原始的本地数据存储而失败。

- 如果您编辑一个池并改变存储永久磁盘和操作系统磁盘的数据存储，View Composer 将无法重新平衡受此改变影响的链接克隆。

  例如，您可能创建一个池并将操作系统磁盘存储在 `datastore1` 中，将 View Composer 永久磁盘存储在 `datastore2` 中。之后，您可能会对池进行编辑，选择 `datastore2` 存储操作系统磁盘，选择 `datastore1` 存储永久磁盘。重新平衡操作无法将操作系统磁盘移至 `datastore2` 或将永久磁盘移至 `datastore1`。

  View Composer 会跳过受影响的链接克隆，只重新平衡不受数据存储改变影响的链接克隆。

重新平衡操作后链接克隆磁盘的文件名

重新平衡链接克隆桌面后，vCenter Server 会更改移到新数据存储中的链接克隆的 View Composer 永久磁盘和一次性数据磁盘的文件名。

原始文件名标识了磁盘类型，重新命名后的磁盘不包括标识标签。

原始的永久磁盘文件名中含有一个 `user-disk` 标签：*桌面名称*`-vdm-user-disk-D-`*`ID`*`.vmdk`。

原始的一次性数据磁盘文件名中含有一个 `disposable` 标签：*桌面名称*`-vdm-disposable-`*`ID`*`.vmdk`。

重新平衡操作将链接克隆移至新数据存储后，vCenter Server 为两种类型的磁盘使用相同的文件名语法：*桌面名称*`_`*`n`*`.vmdk`。

管理 View Composer 永久磁盘

您可以从链接克隆桌面分离 View Composer 永久磁盘，分离磁盘，并将其附加到另一个链接克隆。借助此功能，您可以分开管理用户信息和链接克隆桌面。

将永久磁盘附加到链接克隆桌面时，目标链接克隆必须使用 vSphere 模式。

View Composer 永久磁盘

使用 View Composer，您可以在链接克隆桌面中的不同磁盘上配置操作系统数据和用户信息。更新、刷新或重新平衡操作系统数据时，View Composer 会将用户信息保留在永久磁盘上。

View Composer 永久磁盘包含用户设置和其他由用户生成的数据。

您可以将永久磁盘从其链接克隆桌面分离，并将该磁盘存储到原始数据存储或其他数据存储中。分离此磁盘后，链接克隆虚拟机会随之删除。分离的永久磁盘不再与任何桌面相关联。

将分离的永久磁盘附加到其他链接克隆桌面的方法有多种。这种灵活性优势具有许多用途：

- 您可以在删除链接克隆时保留用户数据。
- 在员工离开公司后，另一位员工可以访问他的用户数据。
- 拥有多个桌面的用户可以将用户数据整合到一个桌面上。
- 如果虚拟机在 vCenter Server 中变得不可访问，但永久磁盘完整无缺，您可以导入永久磁盘并使用此磁盘创建一个新的链接克隆。

注意 您无法从 Windows XP 链接克隆中分离永久磁盘并在 Windows 7 或 Windows Vista 链接克隆中重新创建或附加此永久磁盘。永久磁盘必须重新连接到其创建时所使用的操作系统。

View Manager 能够管理在 View Manager 4.5 中创建的链接克隆池内的永久磁盘。无法管理在早期版本的 View Manager 中创建的永久磁盘，并且这些磁盘不会显示在 View Administrator 的 [Persistent Disks（永久磁盘）] 页面上。

分离 View Composer 永久磁盘

从链接克隆桌面分离 View Composer 永久磁盘时，将存储该磁盘，但会删除链接克隆。通过分离永久磁盘，您可以存储用户相关信息，并在另一个桌面上重新使用这些信息。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Persistent disks（永久磁盘）]**。

2 选择要分离的永久磁盘。

3 单击 **[Detach（分离）]**。

4 选择用来存储永久磁盘的位置。

选项	描述
Use current datastore（使用当前数据存储）	将永久磁盘存储到其当前所在的数据存储。
Move to the following datastore（移到以下数据存储）	选择用来存储永久磁盘的新数据存储。单击 **[Browse（浏览）]**，然后单击向下箭头，从 **[Choose a Datastore（选择数据存储）]** 菜单中选择一个新的数据存储。

5 （可选）单击 **[Save the OS Disk（保存操作系统磁盘）]**，将链接克隆的操作系统磁盘存储到 vCenter Server 中。

您可以检索 vCenter Server 中分离的操作系统磁盘中的数据。但是，该操作系统磁盘不再作为链接克隆桌面存在于 View Manager 中，并且您无法直接从分离的操作系统磁盘重建桌面。保存的操作系统数据中包含基础映像磁盘副本，因此存储的磁盘可能会大于原始的链接克隆操作系统磁盘。

View Composer 永久磁盘保存在数据存储中。链接克隆桌面会被删除，而且不会出现在 View Administrator 中。

将 View Composer 永久磁盘附加到其他链接克隆桌面

您可以将一个分离的永久磁盘附加到另一个链接克隆桌面。附加永久磁盘可使该磁盘中的用户设置和信息供其他桌面的用户使用。

您可以将分离的永久磁盘作为辅助磁盘附加到选定的链接克隆桌面上。新的桌面用户可以访问辅助磁盘，也可以访问桌面上现有的用户信息和设置。

前提条件

- 确认所选桌面是采用 vSphere 模式的池中的一个链接克隆。
- 确认所选桌面与创建永久磁盘的链接克隆使用相同的操作系统。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Persistent disks（永久磁盘）]**。
2 单击 **[Detached（分离的）]** 选项卡。
3 选择永久磁盘。
4 单击 **[Attach（附加）]**。
5 选择要附加永久磁盘的链接克隆桌面。
6 选择 **[Attach as a secondary disk（作为辅助磁盘附加）]**。
7 单击 **[Finish（完成）]**。

下一步

确保链接克隆桌面的用户拥有足够的特权来使用附加的辅助磁盘。例如，如果原始用户对永久磁盘有一定的访问权限，而永久磁盘作为驱动器 D 附加于新桌面，那么，新桌面的用户对驱动器 D 必须拥有和原始用户一样的访问权限。

作为管理员登录桌面的客户操作系统并为新的桌面用户分配适当的特权。

编辑 View Composer 永久磁盘池或用户

如果原始池或用户已从 View Manager 中删除，您可以将分离出的 View Composer 永久磁盘分配给一个新池或用户。

分离的永久磁盘仍与原始池和用户相关联。如果从 View Manager 中删除了池或用户，您无法使用永久磁盘重新创建链接克隆桌面。

通过编辑池和用户，您可以使用分离的永久磁盘在新池中重新创建桌面。桌面会分配给新用户。

您可以选择一个新池、新用户或同时选择两者。

前提条件

- 确认永久磁盘的池或用户已从 View Manager 中删除。
- 确认新池是一个使用 vSphere 模式的链接克隆池。
- 确认新池与创建永久磁盘的池使用相同的操作系统。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Persistent Disks（永久磁盘）]**。
2 选择删除了用户或池的永久磁盘。
3 单击 **[Edit（编辑）]**。

4 （可选）从列表中选择一个链接克隆池。

5 （可选）为永久磁盘选择一个用户。

   您可以浏览 Active Directory 寻找域和用户名。

下一步

使用分离的永久磁盘重建链接克隆桌面。

使用分离的永久磁盘重建链接克隆桌面

分离 View Composer 永久磁盘时会删除链接克隆。您可以通过从分离的磁盘重建链接克隆桌面，授予原始用户访问分离的用户设置和信息的权限。

注意 如果您在已达到最大大小的池中重新创建链接克隆桌面，重新创建的桌面仍然会被添加到池中。该池的大小会增长并超出指定的最大值。

如果某个永久磁盘的原始池或用户已从 View Manager 中删除，您可以为该永久磁盘分配一个新的池或用户。请参阅第 157 页，“编辑 View Composer 永久磁盘池或用户”。

前提条件

确认重新创建链接克隆的桌面池使用了 vSphere 模式。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Persistent Disks（永久磁盘）]**。

2 单击 **[Detached（分离的）]** 选项卡。

3 选择永久磁盘。

   您可以选择多个永久磁盘，以便为每个磁盘创建一个链接克隆桌面。

4 单击 **[Recreate Desktop（重新创建桌面）]**。

5 单击 **[OK（确定）]**。

View Manager 将为您选择的每个永久磁盘创建一个链接克隆桌面，并且将创建的桌面添加到原始池中。

永久磁盘仍然保留在其所在的数据存储中。

通过从 vSphere 导入永久磁盘来还原链接克隆桌面

如果链接克隆桌面配置了 View Composer 永久磁盘，则当它在 View Manager 中变得不可访问时，可以对它进行还原。您可以将永久磁盘从 vSphere 数据存储导入到 View Manager 中。

您可以将永久磁盘文件作为分离的永久磁盘导入到 View Manager 中。然后，可以在 View Manager 中将分离的磁盘附加到现有桌面，或者重建原始的链接克隆。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Persistent Disks（永久磁盘）]**。

2 单击 **[Detached（分离的）]** 选项卡。

3 单击 **[Import from vCenter（从 vCenter 导入）]**。

4 选择一个 vCenter Server。

5 选择磁盘文件所在的数据存储。

6 选择一个链接克隆池，以便使用永久磁盘在其中创建新的链接克隆桌面。

7 在 **[Persistent Disk File（永久磁盘文件）]** 框中，单击 **[Browse（浏览）]**，然后单击向下箭头，从 **[Choose a Datastore（选择数据存储）]** 菜单中选择一个数据存储。

8 单击数据存储名称，显示其磁盘存储文件和虚拟机文件。

9 选择您要导入的永久磁盘文件。

10 在 **[User（用户）]** 框中，单击 **[Browse（浏览）]**，选择要分配给该桌面的用户，然后单击 **[OK（确定）]**。

该磁盘文件会作为分离的永久磁盘导入到 View Manager 中。

下一步

要还原链接克隆桌面，您可以重建原始桌面或者将分离的永久磁盘附加到另一个桌面。

有关详细信息，请参阅第 158 页，“使用分离的永久磁盘重建链接克隆桌面”和第 157 页，“将 View Composer 永久磁盘附加到其他链接克隆桌面”。

删除分离的 View Composer 永久磁盘

删除分离的永久磁盘时，您可以从 View Manager 中移除该磁盘但将其保留在数据存储中；也可以将其从 View Manager 和数据存储中删除。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）]** > **[Persistent Disks（永久磁盘）]**。

2 单击 **[Detached（分离的）]** 选项卡。

3 选择永久磁盘。

4 单击 **[Delete（删除）]**。

5 选择从 View Manager 中移除磁盘后，是从数据存储中删除该磁盘，还是将其保留在数据存储中。

选项	描述
Delete from disk（从磁盘删除）	删除后，永久磁盘将不再存在。
Delete from View Manager only（仅从 View Manager 中删除）	删除后，不能再从 View Manager 访问永久磁盘，但该磁盘仍然保留在数据存储中。

6 单击 **[OK（确定）]**。

管理桌面和桌面池 10

在 View Administrator 中，您可以管理桌面池、虚拟机桌面和桌面会话。

本章讨论了以下主题：

管理桌面池

在 View Administrator 中，您可以编辑、禁用和删除桌面池。

编辑桌面池

您可以编辑现有桌面池，以配置池设置、备用桌面数量、数据存储和自定义规范等设置。

前提条件

熟悉在创建池后可以更改和无法更改的池设置。请参阅第 162 页，“修改现有桌面池的设置”和第 162 页，“现有桌面池的固定设置”。

步骤

1 单击 **[Inventory（清单）] > [Pools（池）]**。
2 选择池。
3 单击 **[Edit（编辑）]**。
4 在 **[Edit *pool_name*（编辑<池名称>）]** 对话框中单击某个选项卡，然后重新配置池选项。
5 单击 **[OK（确定）]**。

修改现有桌面池的设置

创建桌面池之后，您可以更改某些配置设置。

表 10–1 现有桌面池的可编辑设置

配置选项卡	描述
General（常规）	编辑池命名选项。
Pool Settings（池设置）	编辑远程桌面电源策略、显示协议和 Adobe Flash 设置等桌面设置。
Provisioning Settings（部署设置）	编辑池部署选项，并将桌面添加到池中。 此选项卡仅适用于自动池。
vCenter Settings（vCenter 设置）	编辑虚拟机模板或默认基础映像。添加或更改 vCenter Server 实例、ESX 主机或群集、数据存储区及其他 vCenter 功能。 新值仅影响在更改设置后创建的新虚拟机。新设置不会影响现有虚拟机。 此选项卡仅适用于自动池。
Guest Customization（客户机自定义）	选择 Sysprep 自定义规范。 如果使用 QuickPrep 来自定义链接克隆池，您可以更改 Active Directory 域和容器，并指定 QuickPrep 关闭脚本及同步后脚本。 此选项卡仅适用于自动池。

现有桌面池的固定设置

创建桌面池之后，您便无法更改某些配置设置。

表 10–2 现有桌面池的固定设置

设置	描述
Pool type（池类型）	创建自动、手动或终端服务池后，就无法更改池的类型。
User assignment（用户分配）	无法在专用分配和浮动分配之间切换。
Type of virtual machine（虚拟机类型）	无法在完整桌面和链接克隆桌面之间切换。
Pool ID（池 ID）	无法更改池 ID。
Desktop-naming and provisioning method（桌面命名和部署方法）	要将桌面添加到池中，您必须使用创建该池时所使用的部署方法。无法在手动指定桌面名称和使用命名模式之间切换。 如果您手动指定名称，则可以将名称添加到桌面名称列表中。 如果您使用命名模式，则可以提高桌面的最大数量。
vCenter settings（vCenter 设置）	无法更改现有虚拟机的 vCenter 设置。 您可以在 **[Edit *pool_name*（编辑<池名称>）]** 对话框中更改 vCenter 设置，但是更改的值仅影响在更改设置后创建的新虚拟机。
View Composer persistent disks（View Composer 永久磁盘）	在创建无永久磁盘的链接克隆池后，无法配置永久磁盘。
View Composer customization method（View Composer 自定义方法）	如果使用 QuickPrep 或 Sysprep 自定义了链接克隆池，则在池中创建或重构桌面时，无法切换至其他自定义方法。

更改由命名模式部署的自动池的大小

使用命名模式部署自动桌面池时，您可以通过改变桌面的最多数量来增加或减少池的大小。

前提条件

- 确认您是使用命名模式来部署池的。如果您手动指定桌面名称，请参阅第 163 页，“将桌面添加到通过名称列表部署的自动池中”。
- 确认池为自动池。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 选择池，然后单击 **[Edit（编辑）]**。

3 单击 **[Provisioning Settings（部署设置）]** 选项卡。

4 在 **[Max number of desktops（桌面最大数量）]** 框中，键入池中所容纳桌面的新数量。

如果您增加池的大小，则可向池中添加新的桌面，直到达到最大数量。

如果减小浮动分配池的大小，未使用的桌面将被删除。如果登录池的用户数超过了新的最大值，用户注销后，池的容量会减小。

如果减小专用分配池的大小，未分配的桌面将被删除。如果给桌面分配的用户超过了新的最大值，取消用户分配后，池的容量会减小。

注意 当您降低池的大小时，如果当前登录或分配给该池的用户数大于最大数值，桌面的实际数量可能会大于 **[Max number of desktops（桌面最大数量）]**。

将桌面添加到通过名称列表部署的自动池中

要将桌面添加到通过手动指定桌面名称部署的自动池中，您需要提供另一列新的桌面名称。利用此功能，您可以扩展桌面池并继续使用您公司的命名约定。

请按照以下指南手动添加桌面名称：

- 将每个桌面名称键入单独的一行中。
- 桌面名称最多可以包含 15 个字母数字字符。
- 可以为每个桌面条目添加一个用户名。使用逗号来分隔用户名与桌面名称。

以下示例中添加了两个桌面，第二个桌面与一个用户相关联：

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

注意 在浮动分配池中，您不能将用户名与桌面名称相关联。桌面不会专供关联的用户使用。在浮动分配池中，当前未处于使用状态的所有桌面均可供登录的用户访问。

前提条件

确认您是通过手动指定桌面名称来创建池。如果您通过提供命名模式来创建池，则不能通过提供新桌面名称添加桌面。

步骤

1 创建一个包含其他桌面名称列表的文本文件。

如果您仅打算添加几个桌面，则可以直接在 [Add Pool（添加池）] 向导中键入桌面名称，而不必创建单独的文本文件。

2 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

3 选择要扩展的池。

4 单击 **[Edit（编辑）]**。

5 单击 **[Provisioning Settings（部署设置）]** 选项卡。

6 单击 **[Add Desktops（添加桌面）]**。

7 将您的桌面名称列表复制到 [Enter Desktop Names（输入桌面名称）] 页面中，然后单击 **[Next（下一步）]**。

[Enter Desktop Names（输入桌面名称）] 向导将显示桌面列表，并用红色的 **[X]** 来表明验证错误。

8 纠正无效的桌面名称。

a 将鼠标放置在无效名称上方，页面底部会显示相关的错误消息。

b 单击 **[Back（返回）]**。

c 编辑该错误名称，然后单击 **[Next（下一步）]**。

9 单击 **[Finish（完成）]**。

10 单击 **[OK（确定）]**。

View Manager 就会将新桌面添加到池中。

在 vCenter Server 中，您可以监视新虚拟机的创建操作。

在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]** 或 **[Inventory（清单）] > [Desktops（桌面）]**，可以查看添加到池中的桌面。

禁用或启用桌面池

当您禁用某个桌面池时，该池将不再提供给用户。用户无法访问该池。禁用池后，您可以重新启用池。

在准备桌面时，您可以禁用池以防止用户访问他们的桌面。如果不再需要某个池，您可以使用禁用功能撤消池的可用状态，而无需从 View Manager 中删除该池的定义。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 选择一个桌面池并更改池的状态。

选项	操作
禁用池	单击 **[Status（状态）] > [Disable Pool（禁用池）]**。
启用池	单击 **[Status（状态）] > [Enable Pools（启用池）]**。

3 单击 **[OK（确定）]**。

在桌面池中禁用或启用部署

在桌面池中禁用部署后，View Manager 将停止为该池部署新虚拟机。禁用部署后，您可以重新启用部署。

在更改池的配置之前，您可以禁用部署以确保没有用旧配置创建的新桌面。您还可以禁用部署，从而防止 View Manager 在池快要填满可用空间时使用更多存储空间。

当链接克隆池的部署被禁用时，View Manager 会停止部署新桌面以及自定义已重构或已重新平衡的桌面。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 选择一个桌面池并更改池的状态。

选项	操作
禁用部署	单击 **[Status（状态）] > [Disable Provisioning（禁用部署）]**。
启用部署	单击 **[Status（状态）] > [Enable Provisioning（启用部署）]**。

3 单击 **[OK（确定）]**。

从 View Manager 中删除桌面池

从 View Manager 中删除桌面池后，用户将无法访问该池中的桌面。

如果您将虚拟机保留在 vCenter Server 中，当前处于活动会话状态的用户可以继续使用完整的虚拟机桌面。当这些用户注销后，就无法再访问已删除的桌面。

删除链接克隆桌面时，vCenter Server 始终会从磁盘上删除虚拟机。

重要事项 在 View Administrator 中删除桌面池之前，请不要在 vCenter Server 中删除虚拟机。否则可能会使 View 组件处于不一致的状态。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 选择一个桌面池，然后单击 **[Delete（删除）]**。

3 选择如何删除池。

选项	描述
Pool that contains full virtual-machine desktops（包含完整虚拟机桌面的池）	选择在 vCenter Server 中是保留还是删除虚拟机。 如果您从磁盘上删除了虚拟机，处于活动会话中的用户将从其桌面断开。 如果您在 vCenter Server 中保留虚拟机，请选择是允许处于活动会话中的用户与其桌面保持连接还是将他们断开。
Linked-clone pool with View Composer persistent disks（带 View Composer 永久磁盘的链接克隆池）	选择在删除桌面时是分离还是删除永久磁盘。 无论何种情况，vCenter Server 都会从磁盘上删除链接克隆虚拟机。当前处于活动会话中的用户将从其链接克隆桌面断开。 如果分离永久磁盘，则可将该磁盘附加到另一个桌面。您可以将分离的永久磁盘存储在同一个数据存储中，或者存储在不同的数据存储中。 您还可以将操作系统磁盘保存到 vCenter Server 中，以便从这些磁盘中检索数据。每个桌面的操作系统数据保存时都包含基础映像磁盘的副本，因此存储的磁盘可能会大于原始链接克隆操作系统磁盘的大小。
Linked-clone pool without View Composer persistent disks（不带 View Composer 永久磁盘的链接克隆池）	vCenter Server 将从磁盘中删除链接克隆虚拟机。当前处于活动会话中的用户将从其链接克隆桌面断开。

桌面池将从 View Connection Server 中移除。即使您在 vCenter Server 中保留虚拟机，View Manager 也无法访问这些虚拟机。

当您从 View Manager 中删除桌面池时，链接克隆计算机帐户会从 Active Directory 中移除。完整虚拟机帐户仍会保留在 Active Directory 中。要移除这些帐户，您必须从 Active Directory 中手动删除它们。

当您删除包含本地桌面的池时，该桌面的数据中心副本会从 View Manager 中移除。当客户端连接 View Connection Server 或超过与服务器断开连接的最长时间时，本地桌面将不再可用。如果您选择在 vCenter Server 中保留完整虚拟机或分离并保存 View Composer 永久磁盘，那么虚拟机或永久磁盘中将不会保存用户自上一次复制或检出后在本地桌面上所作的更改。

减少 Adobe Flash 带宽

您可以减少 Adobe Flash 内容在 View 桌面会话中运行时使用的带宽。减少带宽可以增强整体浏览体验，并且提高桌面中运行的其他应用程序的响应速度。

配置 Adobe Flash 质量和调节

您可以设置 Adobe Flash 质量和调节模式，以便减少 View 桌面中的 Adobe Flash 内容所使用的带宽量。

前提条件

熟悉 Adobe Flash 的质量和调节设置。请参阅第 166 页，“Adobe Flash 质量和调节”。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 选择一个池，然后单击 **[Edit（编辑）]**。

3 单击 **[Pool Settings（池设置）]** 选项卡。

4 从 **[Adobe Flash quality（Adobe Flash 质量）]** 菜单中选择质量模式。

5 从 **[Adobe Flash throttling（Adobe Flash 调节）]** 菜单中选择调节模式。

6 单击 **[OK（确定）]**。

注意 只有在 View Client 重新连接到桌面后，减少 Adobe Flash 带宽的设置才会生效。

Adobe Flash 质量和调节

您可以为 Adobe Flash 内容指定可重写网页设置的允许的最高质量级别。如果某个网页的 Adobe Flash 质量高于允许的最高级别，则其质量将会降低到指定的最高级别。较低的质量级别可以节省更多的带宽。

要利用减少 Adobe Flash 带宽的设置，不要在全屏幕模式下运行 Adobe Flash。

表 10-3 显示了可用的 Adobe Flash 渲染质量设置。

表 10–3 Adobe Flash 质量设置

质量设置	描述
Do not control（不进行控制）	质量是由网页设置确定的。
Low（低）	此设置节省的带宽最多。
Medium（中）	此设置节省的带宽适中。
High（高）	此设置节省的带宽最少。

如果未指定最高质量级别，则系统默认值为 **[Low（低）]**。

Adobe Flash 使用计时器服务更新任意给定时间在屏幕上显示的内容。典型的 Adobe Flash 计时器间隔值为 4 到 50 毫秒之间。通过调节或延长此间隔，您可以减少帧速率，从而减少带宽。

表 10-4 显示了可用的 Adobe Flash 调节设置。

表 10–4 Adobe Flash 调节设置

调节设置	描述
Disabled（禁用）	不执行调节。不修改计时器间隔。
Conservative（保守）	计时器间隔为 100 毫秒。此设置可以使丢帧数达到最小。
Moderate（中等）	计时器间隔为 500 毫秒。
Aggressive（激进）	计时器间隔为 2500 毫秒。此设置可以使丢帧数达到最大。

无论选择哪种调节设置，音频速度都保持恒定不变。

在终端服务会话中配置 Internet Explorer 中的 Adobe Flash 调节

要确保 Internet Explorer 在终端服务会话中可以使用 Adobe Flash 调节功能，用户必须启用第三方浏览器扩展名。

步骤

1 启动 View Client 并登录到一个用户的桌面。

2 在 Internet Explorer 中，单击 **[Tools（工具）] > [Internet Options（Internet 选项）]**。

3 单击 **[Advanced（高级）]** 选项卡，选择 **[Enable third-party browser extensions（启用第三方浏览器扩展）]**，单击 **[OK（确定）]**。

4 重新启动 Internet Explorer。

在桌面上重写带宽减少设置

使用桌面上的光标，用户可以重写 Adobe Flash 内容显示设置。

步骤

1 在 View 桌面上，启动 Internet Explorer 并浏览到相关的 Adobe Flash 内容。

   如有必要，启动该内容。

   根据 Adobe Flash 的设置配置，您会发现帧丢失或播放质量低。

2 在播放 Adobe Flash 内容时，将光标移动至该内容中。

   只要光标停留在 Adobe Flash 内容中，其显示质量会不断提高。

3 要保持提高的质量，请在 Adobe Flash 内容中双击。

管理虚拟机桌面

您可以搜索、管理和删除虚拟机桌面，还可以管理桌面会话。

查看、断开或重新启动活动会话

您可以查看当前连接到池中 View 桌面的用户，并可以将用户从其桌面断开，强制用户注销以及重新启动活动会话。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pool（池）]**。

2 双击一个池，然后单击 **[Sessions（会话）]** 选项卡。

3 选择一个桌面。

4 选择是断开、注销，还是重新启动会话。

选项	描述
Disconnect Session（断开会话）	将用户从桌面断开。会话仍然保持活动。如果 **[Automatically logoff after disconnect（断开连接后自动注销）]** 设置为 **[Never（从不）]**，或者断开的时间未超过指定的时间长度，用户可以再次登录回该会话。在创建池或创建池后编辑其设置时，可以配置 **[Automatically logoff after disconnect（断开连接后自动注销）]** 设置。
Logoff Session（注销会话）	将用户从桌面断开。用户将注销。
Reset（重置）	在没有正常注销和断开的情况下关闭桌面并重新启动会话。
Send Message（发送消息）	允许您键入一条显示在用户桌面上的消息。

将桌面分配给用户

在专用分配池中，您可以将用户分配为桌面的所有者。只有分配的用户才可以登录并连接到该桌面。

在以下情况下，View Manager 会将桌面分配给用户。

- 当您创建一个池并选择 **[Enable automatic assignment（启用自动分配）]** 设置时。

  注意 如果您选择了 **[Enable automatic assignment（启用自动分配）]** 设置，可以手动将桌面分配给用户。

- 当您创建自动池时，选择 **[Specify desktop names manually（手动指定桌面名称）]** 设置，并提供用户名和桌面名称。

如果您在专用分配池中未选择任何设置，用户将无法访问桌面。必须手动将桌面分配给每个用户。

您可以使用 `vdmadmin` 命令将桌面分配给用户。请参阅第 275 页，“使用 -L 选项分配专用桌面”。

前提条件

- 确认桌面从属于专用分配池。在 View Administrator 中，桌面池页面的 [Settings（设置）] 选项卡中会显示池分配情况。
- 确认桌面没有被检出在本地模式下使用。当桌面处于检出状态时，您无法分配用户或移除用户分配。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Desktops（桌面）]**，或者单击 **[Inventory（清单）] > [Pools（池）]**，然后双击池 ID 并选择 **[Inventory（清单）]** 选项卡。

2 选择桌面。

3 单击 **[More Commands（更多命令）] > [Assign User（分配用户）]**。

4 选择是查找用户还是查找组，选择域，然后在 **[Name（名称）]** 或 **[Description（描述）]** 文本框中键入搜索字符串。

5 选择用户名或组名，然后单击 **[OK（确定）]**。

从专用桌面取消用户分配

在专用分配池中，您可以移除对用户的桌面分配。

您还可以使用 `vdmadmin` 命令来移除对用户的桌面分配。请参阅第 275 页，“使用 -L 选项分配专用桌面”。

前提条件

确认桌面没有被检出在本地模式下使用。当桌面处于检出状态时，您无法分配用户或移除用户分配。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Desktops（桌面）]**，或者单击 **[Inventory（清单）] > [Pools（池）]**，然后双击池 ID 并选择 **[Inventory（清单）]** 选项卡。

2 选择桌面。

3 单击 **[More Commands（更多命令）] > [Unassign User（取消分配用户）]**。

4 单击 **[OK（确定）]**。

该桌面即可供使用，并且可以分配给其他用户。

在维护模式下自定义现有桌面

创建桌面池后，您可以将各个桌面置于维护模式，从而自定义、修改或测试这些桌面。当桌面处于维护模式时，用户无法访问桌面。

您一次只能将一个现有桌面置于维护模式。您可以通过一个操作使多个桌面退出维护模式。

创建池时，如果您手动指定桌面名称，则可以在维护模式下启动该池中的所有桌面。有关详细信息，请参阅第 95 页，“在维护模式下自定义桌面”。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Desktops（桌面）]**，或者单击 **[Inventory（清单）] > [Pools（池）]**，然后双击池 ID 并选择 **[Inventory（清单）]** 选项卡。

2 选择一个桌面。

3 单击 **[More Commands（更多命令）] > [Enter Maintenance Mode（进入维护模式）]**。

4 自定义、修改或测试虚拟机桌面。

5 对您要自定义的所有桌面重复步骤 2 到步骤 4。

6 选择已自定义的桌面，然后单击 **[More Commands（更多命令）] > [Exit Maintenance Mode（退出维护模式）]**。

修改后的桌面即可供用户使用。

监视桌面状态

使用 View Administrator 仪表板可以快速浏览 View 部署中桌面的状态。例如，您可以显示所有断开的桌面或处于维护模式下的桌面。

前提条件

熟悉桌面状态。请参阅第 170 页，“虚拟机的桌面状态”。

步骤

1 在 View Administrator 中，单击 **[Dashboard（仪表板）]**。

2 在 [Desktop Status（桌面状态）] 窗格中，展开一个状态文件夹。

选项	描述
Preparing（正在准备）	列出当虚拟机处于部署、删除或维护模式时的桌面状态。
Problem Desktops（问题桌面）	列出桌面错误状态。
Prepared for use（已准备好，可供使用）	列出当桌面可供使用时的桌面状态。

3 定位桌面状态，并单击旁边带超链接的数字。

[Desktops（桌面）] 页面将显示所有处于选定状态的桌面。

下一步

您可以单击某个桌面名称查看桌面的详细信息，也可以单击 View Administrator 后退箭头返回到仪表板页面。

虚拟机的桌面状态

vCenter Server 管理的虚拟机桌面可处于各种操作和可用性状态下。在 View Administrator 中，您可以在桌面列表页面的右侧列中跟踪桌面的状态。

表 10–5 显示了 View Administrator 中显示的虚拟机桌面操作状态。任何时候，每个桌面都只能处于一种状态下。

表 10–5 vCenter Server 管理的虚拟机桌面的状态

状态	状态类型	描述
Provisioning（部署）	部署	正在部署虚拟机。
Provisioning error（部署错误）	部署	部署过程中发生错误。
Customizing（自定义）	部署	正在自定义自动池中的虚拟机。
Deleting（删除）	部署	虚拟机已标记进行删除。View Manager 很快会删除该虚拟机。
Waiting for Agent（正在等待代理）	代理状态	View Connection Server 正在等待与手动池中的虚拟机上的 View Agent 建立通信。 **注意** 此状态与自动池中虚拟机的 [Customizing（正在自定义）] 状态相同。
Startup（启动）	代理状态	虚拟机上的 View Agent 已经启动，但所需的其他服务（如显示协议等）仍正在启动。例如，直到 RDP 启动完成，View Agent 才能与客户端计算机建立 RDP 连接。
Agent unreachable（无法访问代理）	代理状态	View Connection Server 无法与虚拟机上的 View Agent 建立通信。
Configuration error（配置错误）	代理状态	未启用 RDP 或 PCoIP 等显示协议。
Provisioned（已部署）	可用性	虚拟机关闭。
Available（可用）	可用性	虚拟机处于开启状态，可进行活动连接。在专用池中，虚拟机分配给某个用户，并在用户登录时自动启动。
Checked out（已检出）	会话状态	本地桌面的虚拟机已检出。
Connected（已连接）	会话状态	虚拟机处于活动会话中，与某个 View 客户端具有活动的远程连接。
Disconnected（已断开连接）	会话状态	虚拟机处于活动会话中，但已从 View 客户端断开。

表 10–5 vCenter Server 管理的虚拟机桌面的状态 （续）

状态	状态类型	描述
Unassigned user connected（未分配的用户建立了连接）	其他	已分配用户以外的用户登录了专用池中的虚拟机。 例如，如果管理员启动 vSphere Client、在虚拟机上打开一个控制台并登录，就可能出现此状态。
Unassigned user disconnected（未分配的用户断开连接）	其他	已分配用户以外的用户登录了专用池中的虚拟机并断开了连接。
Unknown（未知）	其他	虚拟机处于未知状态。
Maintenance mode（维护模式）	其他	虚拟机处于维护模式下。用户不能登录或使用该虚拟机。
Error（错误）	其他	虚拟机中发生了未知错误。
-	其他	虚拟机在处于上述任何状态时发生了故障。

当桌面处于特定状态时，可能会显示其他相关状况。View Administrator 会将这些情况作为桌面状态的后缀显示出来。例如，View Administrator 可能会显示 `[Customizing (missing)`（正在自定义（丢失））`]` 状态。

表 10‑6 中列出了这些附加情况。

表 10–6 桌面状态情况

情况	描述
Missing（丢失）	虚拟机在 vCenter Server 中丢失。 通常情况下，vCenter Server 中已删除此虚拟机，但 View LDAP 配置中仍然有该桌面的记录。
Task halted（任务暂停）	View Composer 操作（如刷新、重构或重新平衡）停止。 有关重构操作故障排除的详细信息，请参阅第 152 页，“更正失败的重构”。 有关 View Composer 错误状态的详细信息，请参阅第 263 页，“View Composer 部署错误”。 `[Task halted`（任务暂停）`]` 状况适用于已选为执行此操作的所有虚拟机，但不适用于尚未开始此操作的虚拟机。池中未选为执行此操作的虚拟机不会被置于 `[Task halted`（任务暂停）`]` 状态。

如果 View Composer 任务停止且虚拟机在 vCenter Server 中丢失，桌面就会同时有两种状态，即 `[(missing, task halted)`（丢失，任务暂停）`]`。

从 View Manager 中删除桌面

从 View Manager 中删除桌面后，用户将无法访问这些桌面。

如果您将虚拟机保留在 vCenter Server 中，当前处于活动会话状态的用户可以继续使用完整的虚拟机桌面。当这些用户注销后，就无法再访问已删除的桌面。

删除链接克隆桌面时，vCenter Server 始终会从磁盘上删除虚拟机。

注意 在 View Administrator 中删除桌面之前，请不要在 vCenter Server 中删除虚拟机。否则可能会使 View 组件处于不一致的状态。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Desktops（桌面）]**。

2 选择一个或多个桌面，然后单击 **[Remove（移除）]**。

3 选择如何删除桌面。

选项	描述
Pool that contains full virtual-machine desktops（包含完整虚拟机桌面的池）	选择在 vCenter Server 中是保留还是删除虚拟机。 如果您从磁盘上删除了虚拟机，处于活动会话中的用户将从其桌面断开。 如果您在 vCenter Server 中保留虚拟机，请选择是允许处于活动会话中的用户与其桌面保持连接还是将他们断开。
Linked-clone pool with View Composer persistent disks（带 View Composer 永久磁盘的链接克隆池）	选择在删除桌面时是分离还是删除永久磁盘。 无论何种情况，vCenter Server 都会从磁盘上删除链接克隆虚拟机。当前处于活动会话中的用户将从其链接克隆桌面断开。 如果分离永久磁盘，则可将该磁盘附加到另一个桌面。您可以将分离的永久磁盘存储在同一个数据存储中，或者存储在不同的数据存储中。 您还可以将操作系统磁盘保存到 vCenter Server 中，以便从这些磁盘中检索数据。每个桌面的操作系统数据保存时都包含基础映像磁盘的副本，因此存储的磁盘可能会大于原始链接克隆操作系统磁盘的大小。
Linked-clone pool without View Composer persistent disks（不带 View Composer 永久磁盘的链接克隆池）	vCenter Server 将从磁盘中删除链接克隆虚拟机。当前处于活动会话中的用户将从其链接克隆桌面断开。

桌面将从 View Connection Server 中移除。即使您在 vCenter Server 中保留虚拟机，View Manager 也无法访问这些虚拟机。

当您从 View Manager 中删除桌面时，链接克隆计算机帐户会从 Active Directory 中移除。完整虚拟机帐户仍会保留在 Active Directory 中。要移除这些帐户，您必须从 Active Directory 中手动删除它们。

当您删除本地桌面时，该桌面的数据中心副本会从 View Manager 中移除。当客户端连接 View Connection Server 或超过与服务器断开连接的最长时间时，本地桌面将不再可用。如果您选择在 vCenter Server 中保留完整虚拟机或分离并保存 View Composer 永久磁盘，那么虚拟机或永久磁盘中将不会保存用户自上一次复制或检出后在本地桌面上所作的更改。

将 View 信息导出到外部文件中

在 View Administrator 中，您可以将 View 表信息导出到外部文件中。您可以导出那些列出了用户和用户组、池、桌面、View Composer 永久磁盘、ThinApp 应用程序、事件和 VDI 会话的表。您可以在电子表格或其他工具中查看和管理这些信息。

例如，您可以收集受多个 View Connection Server 实例或副本 View Connection Server 实例组管理的桌面的相关信息。您可以从每个 View Administrator 界面导出 **[Desktops（桌面）]** 表，然后在电子表格中查看此表。

当您导出 View Administrator 表时，它会保存为逗号分隔的 `cvs` 文件。此功能将导出整个表，而不是单个页面。

步骤

1 在 View Administrator 中，显示您要导出的表。

例如，单击 **[Inventory（清单）] > [Desktops（桌面）]** 显示桌面表。

2 单击位于表右上角的 **[Export（导出）]** 图标。

当您将鼠标放在该图标上时，会显示 `Export table contents`（导出表内容）提示信息。

3 在 [Select location for download（选择下载位置）] 对话框中键入 `csv` 文件的文件名。

默认名称是 `global_table_data_export.csv`。

4 浏览到用来存储该文件的位置。

5 单击 **[Save（保存）]**。

下一步

打开电子表格或其他工具来查看该 csv 文件。

管理物理机和终端服务器 11

在 View Administrator 中，您可以添加、移除和取消注册未受 vCenter Server 管理的 View 桌面。未受管的桌面源包括不受 vCenter Server 管理的虚拟机、物理机、刀片 PC 和 Microsoft 终端服务源。

注意 重新配置某个影响未受管桌面源的设置时，新设置最多需要 10 分钟才能生效。例如，如果您更改 [Global Settings（全局设置）] 中的 [Message security mode（消息安全模式）] 或更改池的 [Automatically logoff after disconnect（断开连接后自动注销）] 设置，View Manager 最多可能需要 10 分钟才能重新配置受影响的未受管桌面源。

本章讨论了以下主题：

将未受管桌面源添加到池中

您可以通过向池中添加桌面源来增加使用未受管桌面源的手动桌面池的大小。

前提条件

确认未受管的桌面源上安装了 View Agent。请参阅第 37 页，“在未受管的桌面源中安装 View Agent”。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 在 [Pools（池）] 表的左侧列中，单击手动池的池 ID。

3 在 **[Inventory（清单）]** 选项卡中，单击 **[Add（添加）]**。

4 从 [Add Desktop（添加桌面）] 窗口中选择桌面源，然后单击 **[OK（确定）]**。

View Manager 会将桌面源添加到池中。

从池中移除未受管桌面源

您可以通过从池中移除桌面源来减少使用未受管桌面源的手动桌面池的大小。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 双击池 ID，然后选择 **[Inventory（清单）]** 选项卡。

3 选择要移除的桌面源。

4 单击 **[Remove（移除）]**。

5 如果有用户已登录到未受管的桌面中，请选择是终止其会话，还是允许会话继续活动。

选项	描述
Leave active（保留活动）	活动会话将保留，直到用户注销为止。View Connection Server 不会跟踪这些会话。
Terminate（终止）	立即终止活动会话。

6 单击 **[OK（确定）]**。

View Manager 会从池中移除桌面源。

删除包含未受管桌面的池

当您删除包含未受管桌面源的桌面池时，该池会从 View Manager 中移除。

步骤

1 在 View Administrator 中，单击 **[Inventory（清单）] > [Pools（池）]**。

2 选择一个未受管的桌面池，然后单击 **[Delete（删除）]**。

3 如果有用户已登录到未受管的桌面中，请选择是终止其会话，还是允许会话继续活动。

选项	描述
Leave active（保留活动）	活动会话将保留，直到用户注销为止。View Connection Server 不会跟踪这些会话。
Terminate（终止）	立即终止活动会话。

4 单击 **[OK（确定）]**。

未受管的桌面池就会从 View Manager 中移除。View Manager 不会删除从属于该池的未受管桌面源的注册信息。

要从 View Manager 移除未受管桌面源，您必须取消注册它们。请参阅第 176 页，"取消注册未受管的桌面源"。

取消注册未受管的桌面源

vCenter Server 管理的所有桌面源都在您安装 View Agent 时进行了注册。您仅可取消注册未受管理的桌面源。

未受管的桌面源包括不受 vCenter Server 管理的虚拟机、物理机、刀片 PC 和终端服务源。

如果取消注册桌面源，该桌面源在 View Manager 中将变为不可用。要使某个源重新可用，请在桌面源中重新安装 View Agent。

前提条件

确认您想取消注册的桌面源未被任何桌面池使用。

步骤

1 单击 **[View Configuration（View 配置）] > [Registered desktop sources（已注册的桌面源）]**。

2 选择未受管理的桌面源类型，然后单击 **[Details（详细信息）]**。

3 选择要取消注册的桌面源，并单击 **[Unregister（取消注册）]**。

   您只能选择未被桌面池使用的桌面源。

4 单击 **[OK（确定）]**，确认您要取消注册桌面源。

桌面源已取消注册，并且不再可用。

物理机和终端服务器的桌面状态

物理机、终端服务器或不受 vCenter Server 管理的虚拟机等桌面源可处于各种操作和可用性状态下。在 View Administrator 中，您可以在桌面列表页面的右侧列中跟踪桌面的状态。

表 11‑1 显示了 View Administrator 中显示的物理机和终端服务器桌面的操作状态。任何时候，每个桌面都只能处于一种状态下。

表 11‑1 物理机或终端服务器桌面的状态

状态	状态类型	描述
Waiting for Agent（正在等待代理）	代理状态	View Connection Server 正在等待接收从物理机或终端服务器桌面上的 View Agent 发出的第一条请求。
Agent not reachable（无法访问代理）	代理状态	View Connection Server 无法与桌面上的 View Agent 建立通信。桌面源计算机可能已关机。
Configuration error（配置错误）	代理状态	未启用显示协议（如 RDP），未启用终端服务器，或者未启用其他协议。
Available（可用）	可用性	桌面源计算机已开机，且该桌面可接受活动连接。在专用池中，桌面会分配给某个用户。桌面将在用户登录时启动。
Connected（已连接）	会话状态	桌面处于活动会话中，与某个 View 客户端具有活动的远程连接。
Disconnected（已断开连接）	会话状态	桌面处于活动会话中，但已从 View 客户端断开。
-	其他	桌面在处于上述任何状态时发生了故障。

在 View Administrator 中管理 ThinApp 应用程序

12

您可以使用 View Administrator 分发和管理用 VMware ThinApp™ 打包的应用程序。在 View Administrator 中管理 ThinApp 应用程序的任务包括：捕获和存储应用程序包、将 ThinApp 应用程序添加到 View Administrator 以及将 ThinApp 应用程序分配到桌面和池。

您必须拥有在 View Administrator 中使用 ThinApp 管理功能的许可。

本章讨论了以下主题：

View 对 ThinApp 应用程序的要求

在 View Administrator 中捕获和存储要分发到 View 桌面的 ThinApp 应用程序时，必须满足某些要求。

- 必须将应用程序打包为 Microsoft Installation (MSI) 包。
- 必须使用 ThinApp 4.6 或更高版本来创建 MSI 包。
- 必须将 MSI 包存储到 Windows 网络共享位置，该共享位置必须位于 View Connection Server 主机和 View 桌面均可访问的 Active Directory 域中。文件服务器必须支持基于计算机帐户的身份验证和文件权限。
- 必须在托管 MSI 包的网络共享位置上配置文件和共享权限，为内置 Active Directory 组 "Domain Computers" 授予读访问权限。如果您打算将 ThinApp 应用程序分发给域控制器，还必须为内置 Active Directory 组 "Domain Controllers" 授予读访问权限。
- 确保非连续命名空间不会阻止域成员计算机访问托管 MSI 包的网络共享位置。当 Active Directory 域名和该域中计算机使用的 DNS 命名空间不同时，将会出现非连续命名空间。有关更多信息，请参阅 VMware 知识库 (KB) 文章 1023309。
- 要在 View 桌面上运行流式 ThinApp 应用程序，用户必须有权访问托管 MSI 包的网络共享位置。

捕获和存储应用程序包

ThinApp 通过可将应用程序从底层操作系统及其库和框架中分离，并将应用程序捆绑到一个可执行文件（称为应用程序包）来提供应用程序虚拟化。

要在 View Administrator 中管理 ThinApp 应用程序，您必须使用 ThinApp [Setup Capture（安装捕获）] 向导以 MSI 格式捕获并打包应用程序，并且将 MSI 程序包存储在应用程序存储库中。

应用程序存储库是一个 Windows 网络共享位置。您可以使用 View Administrator 将网络共享位置注册为应用程序存储库。您可以注册多个应用程序存储库。

注意 如果您拥有多个应用程序存储库，则必须使用第三方解决方案来管理负载平衡和可用性。View 中不包含负载平衡或可用性解决方案。

有关 ThinApp 功能以及如何使用 ThinApp [Setup Capture（安装捕获）] 向导的完整信息，请参阅《*Introduction to VMware ThinApp*》（VMware ThinApp 说明）和《*ThinApp User's Guide*》（ThinApp 用户指南）。

1 将应用程序打包第 180 页，

   您可以使用 ThinApp [Setup Capture（安装捕获）] 向导来捕获和打包应用程序。

2 创建 Windows 网络共享位置第 181 页，

   您必须创建一个 Windows 网络共享位置，以托管在 View Administrator 中分发到 View 桌面和池的 MSI 包。

3 注册应用程序存储库第 181 页，

   您必须在 View Administrator 中将用来托管 MSI 包的 Windows 网络共享位置注册为应用程序存储库。

4 将 ThinApp 应用程序添加到 View Administrator 第 181 页，

   您可以通过扫描应用程序存储库并选择 ThinApp 应用程序将 ThinApp 应用程序添加到 View Administrator 中。将 ThinApp 应用程序添加到 View Administrator 之后，您可以将其分配到桌面和池。

5 创建 ThinApp 模板第 182 页，

   您可以在 View Administrator 中创建一个模板以指定一组 ThinApp 应用程序。您可以使用模板并按照功能、供应商或其他任何适合您组织的逻辑分组方式对应用程序进行整体分组。

将应用程序打包

您可以使用 ThinApp [Setup Capture（安装捕获）] 向导来捕获和打包应用程序。

前提条件

- 从 http://www.vmware.com/cn/products/thinapp 下载 ThinApp 软件，并将其安装到干净的计算机上。View 支持 ThinApp 4.6 及更高版本。
- 熟悉《*ThinApp User's Guide*》（ThinApp 用户指南）中的 ThinApp 软件要求和应用程序打包说明。

步骤

1 启动 ThinApp [Setup Capture（安装捕获）] 向导，按照向导中的提示操作。

2 当 ThinApp [Setup Capture（安装捕获）] 向导提示您指定项目位置时，请选择 **[Build MSI package（生成 MSI 包）]**。

ThinApp [Setup Capture（安装捕获）] 向导会将应用程序、运行该应用程序所需的全部必需组件以及应用程序本身封装到一个 MSI 包中。

下一步

创建一个用于存储 MSI 包的 Windows 网络共享位置。

创建 Windows 网络共享位置

您必须创建一个 Windows 网络共享位置，以托管在 View Administrator 中分发到 View 桌面和池的 MSI 包。

前提条件

- 使用 ThinApp [Setup Capture（安装捕获）] 向导来打包应用程序。
- 确认网络共享位置满足 View 对于存储 ThinApp 应用程序的要求。有关更多信息，请参阅第 179 页，“View 对 ThinApp 应用程序的要求”。

步骤

1. 在 View Connection Server 主机和 View 桌面均可访问的 Active Directory 域中的某个计算机上创建一个共享文件夹。
2. 在共享文件夹上配置文件和共享权限，为内置 Active Directory 组 "Domain Computers" 授予读访问权限。
3. 如果您打算将 ThinApp 应用程序分配到域控制器，必须为内置 Active Directory 组 "Domain Controllers" 授予读访问权限。
4. 将 MSI 包复制到共享文件夹中。

下一步

在 View Administrator 中将 Windows 网络共享位置注册为应用程序存储库。

注册应用程序存储库

您必须在 View Administrator 中将用来托管 MSI 包的 Windows 网络共享位置注册为应用程序存储库。

您可以注册多个应用程序存储库。

前提条件

创建 Windows 网络共享位置。

步骤

1. 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [ThinApp Configuration（ThinApp 配置）]**，然后单击 **[Add Repository（添加存储库）]**。
2. 在 **[Display name（显示名称）]** 文本框中键入应用程序存储库的显示名称。
3. 在 **[Share path（共享路径）]** 文本框中键入托管应用程序包的 Windows 网络共享位置的路径。

   网络共享位置的路径必须是 *服务器计算机名**共享名称* 格式，其中*服务器计算机名*是服务器计算机的 DNS 名称。不要指定 IP 地址。

   例如：`\\server.domain.com\MSIPackages`
4. 单击 **[Save（保存）]** 在 View Administrator 中注册应用程序存储库。

将 ThinApp 应用程序添加到 View Administrator

您可以通过扫描应用程序存储库并选择 ThinApp 应用程序将 ThinApp 应用程序添加到 View Administrator 中。将 ThinApp 应用程序添加到 View Administrator 之后，您可以将其分配到桌面和池。

前提条件

在 View Administrator 中注册应用程序存储库。

步骤

1 在 View Administrator 中，选择 **[Inventory（清单）] > [ThinApp]**。

2 在 **[Summary（摘要）]** 选项卡上，单击 **[Scan New ThinApps（扫描新 ThinApp）]**。

3 选择要扫描的应用程序存储库和文件夹并单击 **[Next（下一步）]**。

   如果应用程序存储库包含子文件夹，可展开根文件夹并选择一个子文件夹。

4 选择您想添加到 View Administrator 的 ThinApp 应用程序。

   您可以使用按住 Ctrl 键并单击或按住 Shift 键并单击的方式选择多个 ThinApp 应用程序。

5 单击 **[Scan（扫描）]** 开始扫描您选择的 MSI 包。

   如果您需要停止扫描，请单击 **[Stop Scan（停止扫描）]**。

   View Administrator 会报告每个扫描操作的状态以及添加到 View Administrator 的 ThinApp 应用程序数量。如果您选择某个已存在于 View Administrator 中的应用程序，则不会再次添加该程序。

6 单击 **[Finish（完成）]**。

   新的 ThinApp 应用程序会显示在 **[Summary（摘要）]** 选项卡上。

下一步

（可选）创建 ThinApp 模板。

创建 ThinApp 模板

您可以在 View Administrator 中创建一个模板以指定一组 ThinApp 应用程序。您可以使用模板并按照功能、供应商或其他任何适合您组织的逻辑分组方式对应用程序进行整体分组。

ThinApp 模板可简化多个应用程序的分发。将 ThinApp 模板分配到桌面或池时，View Administrator 会安装模板中当前所有的应用程序。

创建 ThinApp 模板是可选操作。

注意 如果您在将 ThinApp 模板分配到桌面或池之后向该模板添加应用程序，View Administrator 不会自动将新应用程序分配到桌面或池。如果您从之前分配到桌面或池的 ThinApp 模板中移除应用程序，则该应用程序仍会分配到该桌面或池。

前提条件

将所选的 ThinApp 应用程序添加到 View Administrator 中。

步骤

1 在 View Administrator 中，选择 **[Inventory（清单）] > [ThinApp]**，然后单击 **[New Template（新建模板）]**。

2 键入模板的名称并单击 **[Add（添加）]**。

   所有可用的 ThinApp 应用程序都显示在该表中。

3 要查找一个特定的 ThinApp 应用程序，需要在 **[Find（查找）]** 文本框中键入应用程序名并单击 **[Find（查找）]**。

4 选择您想在模板中包含的 ThinApp 应用程序并单击 **[Add（添加）]**。

   您可以使用按住 Ctrl 键并单击或按住 Shift 键并单击的方式选择多个应用程序。

5 单击 **[OK（确定）]** 保存模板。

将 ThinApp 应用程序分配到桌面和池

要在 View 桌面上安装 ThinApp 应用程序，可以使用 View Administrator 将 ThinApp 应用程序分配到桌面或池。

在您将 ThinApp 应用程序分配到桌面几分钟后，View Administrator 即会开始在该桌面上安装应用程序。当您将 ThinApp 应用程序分配到桌面池中时，View Administrator 会在用户首次登录到该池中的桌面时开始安装该应用程序。

Streaming（流式） View Administrator 将指向 ThinApp 应用程序的快捷方式安装到桌面。该快捷方式指向托管存储库的网络共享位置上的 ThinApp 应用程序。用户必须有权访问该网络共享位置才能运行流式 ThinApp 应用程序。

Full（完整） View Administrator 在本地文件系统中安装完整的 ThinApp 应用程序。

安装 ThinApp 应用程序所花费的时间取决于该应用程序的大小。

重要事项 您仅可以将 ThinApp 应用程序分配到桌面和具有虚拟机源的桌面池。您无法将 ThinApp 应用程序分配到终端服务器、刀片 PC 和传统 PC。

分配 ThinApp 应用程序的最佳实践

将 ThinApp 应用程序分配到桌面和池时，请遵循最佳实践。

- 要在特定桌面上安装 ThinApp 应用程序，请将该应用程序分配到桌面。如果您对桌面使用了通用命名约定，则可以根据桌面分配快速为使用该命名约定的所有桌面分发应用程序。
- 要在池中的所有桌面上安装 ThinApp 应用程序，请将该应用程序分配到池。如果您按部门或用户类型组织池，则可以根据池分配快速为特定部门或用户分发应用程序。例如，如果为会计部门的用户创建了一个池，您可以通过将应用程序分配到该会计池，为会计部门中的所有用户分发同一个应用程序。
- 要简化对多个 ThinApp 应用程序的分发，可以在 ThinApp 模板中包含这些应用程序。将 ThinApp 模板分配到桌面或池后，View Administrator 会安装模板中当前所有的应用程序。

- 如果 ThinApp 模板包含已分配到桌面或池的 ThinApp 应用程序，则不要将该模板分配到该桌面或池。此外，不要通过不同安装类型将 ThinApp 模板多次分配到同一桌面或池。在这两种情况下，View Administrator 将返回 ThinApp 分配错误。
- 尽管不支持将 ThinApp 应用程序分配到本地桌面，但 View Administrator 不会阻止这种操作。如果您想试验将 ThinApp 应用程序分配到本地桌面，则必须满足一定的要求。有关更多信息，请参阅《*VMware View 体系结构规划指南*》。

将一个 ThinApp 应用程序分配到多个桌面

您可以将一个特定的 ThinApp 分配到一个或多个桌面。

前提条件

扫描应用程序存储库，将选定的 ThinApp 应用程序添加到 View Administrator 中。请参阅第 181 页，“将 ThinApp 应用程序添加到 View Administrator”。

步骤

1 选择 **[Inventory（清单）] > [ThinApp]**，然后选择该 ThinApp 应用程序。

2 在 **[Add Assignment（添加分配）]** 下拉菜单中，选择 **[Desktops（桌面）]**。

尚未分配 ThinApp 应用程序的桌面会显示在表中。

选项	操作
查找特定桌面	在 **[Find（查找）]** 文本框中键入桌面名称并单击 **[Find（查找）]**。
查找遵循同一命名约定的所有桌面	在 **[Find（查找）]** 文本框中键入部分桌面名称并单击 **[Find（查找）]**。

3 选择您希望分配 ThinApp 应用程序的桌面并单击 **[Add（添加）]**。

您可以使用按住 Ctrl 键并单击或按住 Shift 键并单击的方式选择多个桌面。

4 选择安装类型，然后单击 **[OK（确定）]**。

选项	操作
Streaming（流式）	在桌面上安装应用程序的快捷方式。该快捷方式指向托管存储库的网络共享位置上的应用程序。用户必须有权访问该网络共享位置才能运行该应用程序。
Full（完整）	在本地文件系统中安装完整的应用程序。

某些 ThinApp 应用程序不支持这两种安装类型。应用程序包的创建方式决定可用的安装类型。

View Administrator 在几分钟后开始安装 ThinApp 应用程序。安装完成后，应用程序即可供桌面的所有用户使用。

将多个 ThinApp 应用程序分配到一个桌面

您可以将一个或多个 ThinApp 应用程序分配给一个特定的桌面。

前提条件

扫描应用程序存储库，将选定的 ThinApp 应用程序添加到 View Administrator 中。请参阅第 181 页，“将 ThinApp 应用程序添加到 View Administrator”。

步骤

1 选择 **[Inventory（清单）] > [Desktops（桌面）]**，然后在 [Desktop（桌面）] 列中双击桌面的名称。

2 在 **[Summary（摘要）]** 选项卡上的 [ThinApp] 窗格中，单击 **[Add Assignment（添加分配）]**。

尚未被分配给桌面的 ThinApp 应用程序将显示在表中。

3 要查找一个特定的应用程序，请在 **[Find（查找）]** 文本框中键入应用程序名并单击 **[Find（查找）]**。

4 选择一个要分配到桌面的 ThinApp 应用程序并单击 **[Add（添加）]**。

重复该步骤添加多个应用程序。

5 选择安装类型，然后单击 **[OK（确定）]**。

选项	操作
Streaming（流式）	在桌面上安装应用程序的快捷方式。该快捷方式指向托管存储库的网络共享位置上的应用程序。用户必须有权访问该网络共享位置才能运行该应用程序。
Full（完整）	在本地文件系统中安装完整的应用程序。

某些 ThinApp 应用程序不支持这两种安装类型。应用程序包的创建方式决定可用的安装类型。

View Administrator 在几分钟后开始安装 ThinApp 应用程序。安装完成后，这些应用程序即可供桌面的所有用户使用。

将一个 ThinApp 应用程序分配到多个池

您可以将某个特定的 ThinApp 应用程序分配到一个或多个池。

将 ThinApp 应用程序分配到链接克隆池时，如果随后刷新、重构或重新平衡该池，则 View Administrator 将重新安装该应用程序。您无需手动重新安装该应用程序。

前提条件

扫描应用程序存储库，将选定的 ThinApp 应用程序添加到 View Administrator 中。请参阅第 181 页，“将 ThinApp 应用程序添加到 View Administrator”。

步骤

1 选择 **[Inventory（清单）] > [ThinApp]**，然后选择该 ThinApp 应用程序。

2 在 **[Add Assignment（添加分配）]** 下拉菜单中，选择 **[Pools（池）]**。

尚未分配 ThinApp 应用程序的池会显示在表中。

选项	操作
查找特定池	在 **[Find（查找）]** 文本框中键入池名称并单击 **[Find（查找）]**。
查找遵循同一命名约定的所有池	在 **[Find（查找）]** 文本框中键入部分池名称并单击 **[Find（查找）]**。

3 选择您希望分配 ThinApp 应用程序的池并单击 **[Add（添加）]**。

您可以使用按住 Ctrl 键并单击或按住 Shift 键并单击的方式选择多个池。

4 选择安装类型，然后单击 **[OK（确定）]**。

选项	操作
Streaming（流式）	在桌面上安装应用程序的快捷方式。该快捷方式指向托管存储库的网络共享位置上的应用程序。用户必须有权访问该网络共享位置才能运行该应用程序。
Full（完整）	在本地文件系统中安装完整的应用程序。

某些 ThinApp 应用程序不支持这两种安装类型。应用程序包的创建方式决定可用的安装类型。

View Administrator 会在用户首次登录到池中桌面时开始安装 ThinApp 应用程序。安装完成后，该应用程序即可供桌面的所有用户使用。

将多个 ThinApp 应用程序分配到一个池

您可以将一个或多个 ThinApp 应用程序分配给一个特定的池。

将 ThinApp 应用程序分配到链接克隆池时，如果随后刷新、重构或重新平衡该池，则 View Administrator 将重新安装该应用程序。您无需手动重新安装该应用程序。

前提条件

扫描应用程序存储库，将选定的 ThinApp 应用程序添加到 View Administrator 中。请参阅第 181 页，“将 ThinApp 应用程序添加到 View Administrator”。

步骤

1 选择 **[Inventory（清单）] > [Pools（池）]**，然后双击池 ID。

2 在 **[Inventory（清单）]** 选项卡上，单击 **[ThinApp]**，然后单击 **[Add Assignment（添加分配）]**。

   尚未被分配到池的 ThinApp 应用程序将显示在表中。

3 要查找某个特定的应用程序，请在 **[Find（查找）]** 文本框中键入 ThinApp 应用程序名并单击 **[Find（查找）]**。

4 选择一个要分配到池的 ThinApp 应用程序并单击 **[Add（添加）]**。

   重复该步骤可选择多个应用程序。

5 选择安装类型，然后单击 **[OK（确定）]**。

选项	操作
Streaming（流式）	在桌面上安装应用程序的快捷方式。该快捷方式指向托管存储库的网络共享位置上的应用程序。用户必须有权访问该网络共享位置才能运行该应用程序。
Full（完整）	在本地文件系统中安装完整的应用程序。

   某些 ThinApp 应用程序不支持这两种安装类型。应用程序包的创建方式决定可用的安装类型。

View Administrator 会在用户首次登录到池中桌面时开始安装 ThinApp 应用程序。安装完成后，这些应用程序即可供桌面的所有用户使用。

将 ThinApp 模板分配到桌面或池

通过将 ThinApp 模板分配到桌面或池，可以简化多个 ThinApp 应用程序的分配。

将 ThinApp 模板分配到桌面或池时，View Administrator 会安装模板中当前所包含的 ThinApp 应用程序。

前提条件

创建 ThinApp 模板。请参阅第 182 页，“创建 ThinApp 模板”。

步骤

1 在 View Administrator 中，选择 **[Inventory（清单）] > [ThinApp]**。

2 选择 ThinApp 模板。

3 在 **[Add Assignment（添加分配）]** 下拉菜单中，选择 **[Desktops（桌面）]** 或 **[Pools（池）]**。

所有桌面或池都将显示在表中。

选项	操作
查找特定桌面或池	在 **[Find（查找）]** 文本框中键入桌面或池名称并单击 **[Find（查找）]**。
查找遵循同一命名约定的所有桌面或池	在 **[Find（查找）]** 文本框中键入部分桌面或池名称并单击 **[Find（查找）]**。

4 选择您希望分配 ThinApp 模板的桌面或池并单击 **[Add（添加）]**。

重复此步骤可选择多个桌面或池。

5 选择安装类型，然后单击 **[OK（确定）]**。

选项	操作
Streaming（流式）	在桌面上安装应用程序的快捷方式。该快捷方式指向托管存储库的网络共享位置上的应用程序。用户必须有权访问该网络共享位置才能运行该应用程序。
Full（完整）	在本地文件系统中安装完整的应用程序。

某些 ThinApp 应用程序不支持这两种安装类型。应用程序包的创建方式决定可用的安装类型。

将 ThinApp 模板分配到桌面几分钟后，View Administrator 即会开始安装模板中的应用程序。将 ThinApp 模板分配到池时，View Administrator 会在用户首次登录到该池中的桌面时开始安装应用程序。安装完成后，这些应用程序即可供桌面或池的所有用户使用。

如果 ThinApp 模板包含已分配到桌面或池的应用程序，View Administrator 会返回一个应用程序分配错误。

查看 ThinApp 应用程序分配

您可以查看当前分配了某个特定 ThinApp 应用程序的所有桌面和池，也可以查看分配给某个特定桌面和池的所有 ThinApp 应用程序。

前提条件

熟悉第 188 页，“ThinApp 应用程序安装状态值”中的 ThinApp 安装状态值。

步骤

◆ 选择您希望查看的 ThinApp 应用程序分配。

选项	操作
查看分配了某个特定 ThinApp 应用程序的所有桌面和池	选择 **[Inventory（清单）]** > **[ThinApp]**，然后双击 ThinApp 应用程序的名称。 **[Assignments（分配）]** 选项卡会显示当前分配了该应用程序的桌面和池，包括安装类型。 **[Desktops（桌面）]** 选项卡会显示当前与该应用程序相关联的桌面，包括安装状态信息。 **注意** 将 ThinApp 应用程序分配到桌面池时，池中的桌面只会在安装了应用程序后才显示在 **[Desktops（桌面）]** 选项卡上。
查看分配给特定桌面的所有 ThinApp 应用程序	选择 **[Inventory（清单）]** > **[Desktops（桌面）]**，然后在 [Desktop（桌面）] 列中双击桌面名称。 **[Summary（摘要）]** 选项卡上的 [ThinApp] 窗格将显示当前分配给该桌面的每个应用程序，包括安装状态。
查看分配给特定池的所有 ThinApp 应用程序	选择 **[Inventory（清单）]** > **[Pools（池）]**，双击池 ID，然后选择 **[Inventory（清单）]** 选项卡并单击 **[ThinApp]**。 [ThinApp Assignments（ThinApp 分配）] 窗格会显示当前分配给该池的每个应用程序。

ThinApp 应用程序安装状态值

将 ThinApp 应用程序分配到桌面或池后，View Administrator 将指示安装的状态。

表 12–1 中描述了各个状态值。

表 12–1 ThinApp 应用程序安装状态

状态	描述
Assigned（已分配）	ThinApp 应用程序已分配到桌面。
Install Error（安装错误）	View Administrator 尝试安装 ThinApp 应用程序时发生错误。
Uninstall Error（卸载错误）	View Administrator 尝试卸载 ThinApp 应用程序时发生错误。
Installed（已安装）	ThinApp 应用程序已安装。
Pending Install（正在等待安装）	View Administrator 正在尝试安装 ThinApp 应用程序。 您不能取消分配处于此状态的应用程序。 **注意** 池中的桌面不会显示此值。
Pending Uninstall（正在等待卸载）	View Administrator 正在尝试卸载 ThinApp 应用程序。

显示 MSI 包信息

将 ThinApp 应用程序添加到 View Administrator 后，您可以显示有关其 MSI 包的信息。

步骤

1 在 View Administrator 中，选择 **[Inventory（清单）] > [ThinApp]**。

  [Summary（摘要）] 选项卡列出了当前可用的应用程序，并显示了完整分配和流式分配的数量。

2 在 ThinApp 列中双击应用程序名。

3 选择 **[Summary（摘要）]** 选项卡查看有关 MSI 包的常规信息。

4 单击 **[Package Info（程序包信息）]** 查看有关 MSI 包的详细信息。

在 View Administrator 中维护 ThinApp 应用程序

在 View Administrator 中维护 ThinApp 应用程序时涉及的任务包括：移除 ThinApp 应用程序分配、移除 ThinApp 应用程序和应用程序存储库，以及修改和删除 ThinApp 模板。

注意 要升级 ThinApp 应用程序，必须先取消分配并移除旧版应用程序，然后再添加并分配新版程序。

- 从多个桌面移除一个 ThinApp 应用程序分配第 189 页，

  您可以从一个或多个桌面移除某个特定的 ThinApp 应用程序分配。

- 从一个桌面移除多个 ThinApp 应用程序分配第 189 页，

  您可以从某个特定桌面移除一个或多个 ThinApp 应用程序分配。

- 从多个池移除一个 ThinApp 应用程序分配第 189 页，

  您可以从一个或多个池移除某个特定的 ThinApp 应用程序分配。

- 从一个池移除多个 ThinApp 应用程序分配第 190 页，

  您可以从某个特定的池中移除一个或多个 ThinApp 应用程序分配。

- 从 View Administrator 中移除 ThinApp 应用程序第 190 页，

  从 View Administrator 中移除 ThinApp 应用程序后，您就不能再将该应用程序分配到桌面和池。

- 修改或删除 ThinApp 模板第 190 页，

  您可以从 ThinApp 模板添加和移除应用程序，也可以删除 ThinApp 模板。

- 移除应用程序存储库第 191 页，

  您可以从 View Administrator 中移除应用程序存储库。

从多个桌面移除一个 ThinApp 应用程序分配

您可以从一个或多个桌面移除某个特定的 ThinApp 应用程序分配。

前提条件

通知相应桌面用户您打算移除应用程序。

步骤

1 选择 **[Inventory（清单）] > [ThinApp]**，然后双击 ThinApp 的名称。

2 在 **[Assignments（分配）]** 选项卡上，选择一个桌面并单击 **[Remove Assignment（移除分配）]**。

   您可以使用按住 Ctrl 键并单击或按住 Shift 键并单击的方式选择多个桌面。

View Administrator 在几分钟后卸载 ThinApp 应用程序。

从一个桌面移除多个 ThinApp 应用程序分配

您可以从某个特定桌面移除一个或多个 ThinApp 应用程序分配。

前提条件

通知相应桌面用户您打算移除应用程序。

步骤

1 选择 **[Inventory（清单）] > [Desktops（桌面）]**，然后在 [Desktop（桌面）] 列中双击桌面的名称。

2 在 **[Summary（摘要）]** 选项卡的 [ThinApp] 窗格中，选择 ThinApp 应用程序并单击 **[Remove Assignment（移除分配）]**。

   重复该步骤移除其他应用程序分配。

View Administrator 在几分钟后卸载 ThinApp 应用程序。

从多个池移除一个 ThinApp 应用程序分配

您可以从一个或多个池移除某个特定的 ThinApp 应用程序分配。

前提条件

通知相应池中的桌面用户您打算移除应用程序。

步骤

1 选择 **[Inventory（清单）] > [ThinApp]**，然后双击 ThinApp 应用程序名称。

2 在 **[Assignments（分配）]** 选项卡上，选择一个池并单击 **[Remove Assignments（移除分配）]**。

   您可以使用按住 Ctrl 键并单击或按住 Shift 键并单击的方式选择多个池。

View Administrator 会在用户首次登录池中的桌面时卸载 ThinApp 应用程序。

从一个池移除多个 ThinApp 应用程序分配

您可以从某个特定的池中移除一个或多个 ThinApp 应用程序分配。

前提条件

通知相应池中的桌面用户您打算移除应用程序。

步骤

1 选择 **[Inventory（清单）] > [Pools（池）]**，然后双击池的 ID。

2 在 **[Inventory（清单）]** 选项卡上，单击 **[ThinApp]**，选择 ThinApp 应用程序，然后单击 **[Remove Assignment（移除分配）]**。

   重复该步骤移除多个应用程序。

View Administrator 会在用户首次登录到池中的桌面时卸载 ThinApp 应用程序。

从 View Administrator 中移除 ThinApp 应用程序

从 View Administrator 中移除 ThinApp 应用程序后，您就不能再将该应用程序分配到桌面和池。

如果您的组织决定用其他供应商的应用程序来取代某个 ThinApp 应用程序，您可能需要移除该 ThinApp 应用程序。

注意 如果某个 ThinApp 应用程序已被分配到桌面或池，或者处于 [Pending Uninstall（正在等待卸载）] 状态，您将无法移除该 ThinApp 应用程序。

前提条件

如果 ThinApp 应用程序当前已被分配到桌面或池，请从该桌面或池移除分配。

步骤

1 在 View Administrator 中，选择 **[Inventory（清单）] > [ThinApp]**，然后选择 ThinApp 应用程序。

2 单击 **[Remove ThinApp（移除 ThinApp）]**。

3 单击 **[OK（确定）]**。

修改或删除 ThinApp 模板

您可以从 ThinApp 模板添加和移除应用程序，也可以删除 ThinApp 模板。

如果您在将 ThinApp 模板分配到桌面或池之后向该模板添加应用程序，View Administrator 不会自动将新应用程序分配到桌面或池。如果您从之前分配到桌面或池的 ThinApp 模板中移除应用程序，则该应用程序仍会分配到该桌面或池。

步骤

◆ 在 View Administrator 中，选择 **[Inventory（清单）] > [ThinApp]**，然后选择 ThinApp 模板。

选项	操作
从模板添加或移除 ThinApp 应用程序	单击 **[Edit Template（编辑模板）]**。
删除模板	单击 **[Delete Template（删除模板）]**。

移除应用程序存储库

您可以从 View Administrator 中移除应用程序存储库。

如果不再需要应用程序存储库中包含的 MSI 包，或者需要将 MSI 包移到其他网络共享位置，您可能需要移除应用程序存储库。您无法在 View Administrator 中编辑应用程序存储库的共享路径。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [ThinApp Configuration（ThinApp 配置）]**，然后选择应用程序存储库。

2 单击 **[Remove Repository（移除存储库）]**。

在 View Administrator 中监视 ThinApp 应用程序并进行故障排除

View Administrator 会将与 ThinApp 应用程序管理相关的事件记录到事件和报告数据库中。您可以在 View Administrator 中的 **[Events（事件）]** 选项卡上查看这些事件。

出现以下情况时，**[Events（事件）]** 选项卡上会显示事件。

- 分配了 ThinApp 应用程序或移除了应用程序分配
- 在桌面上安装或卸载了 ThinApp 应用程序
- 无法安装或卸载 ThinApp 应用程序
- 在 View Administrator 中注册、修改或移除了 ThinApp 应用程序存储库
- 将 ThinApp 应用程序添加到了 View Administrator 中

故障排除提示可帮助您解决常见的 ThinApp 应用程序管理问题。

无法注册应用程序存储库

您无法在 View Administrator 中注册应用程序存储库。

问题

尝试在 View Administrator 中注册应用程序存储库时，收到一条错误消息。

原因

View Connection Server 主机无法访问托管应用程序存储库的网络共享位置。您在 **[Share path（共享路径）]** 文本框中键入的网络共享路径可能不正确，托管应用程序存储库的网络共享位置位于 View Connection Server 主机无法访问的域中，或者尚未正确设置网络共享位置的权限。

解决方案

- 如果网络共享路径不正确，则需要键入正确的网络共享路径。不支持包含 IP 地址的网络共享路径。
- 如果网络共享位置位于不可访问的域中，请将应用程序包复制到 View Connection Server 主机可访问域中的网络共享位置。
- 确认在共享文件夹上的文件和共享权限中为内置 Active Directory 组 "Domain Computers" 授予了读访问权限。如果您打算将 ThinApp 分配到域控制器，请确认在文件和共享权限中为内置 Active Directory 组 "Domain Controllers" 授予了读访问权限。设置或更改权限后，可能需要等待 20 分钟才可以访问网络共享位置。

无法将 ThinApp 应用程序添加到 View Administrator

View Administrator 无法将 ThinApp 应用程序添加到 View Administrator。

问题

在 View Administrator 中单击 **[Scan New ThinApps（扫描新 ThinApp）]** 时，没有可用的 MSI 包。

原因

原因可能在于应用程序包不是 MSI 格式，或者 View Connection Server 主机无法访问网络共享位置中的目录。

解决方案

- 确认应用程序存储库中的应用程序包采用了 MSI 格式。
- 确认网络共享位置满足 View 对于 ThinApp 应用程序的要求。有关更多信息，请参阅第 179 页，"View 对 ThinApp 应用程序的要求"。
- 确认网络共享位置中的目录具有正确的权限。有关更多信息，请参见第 191 页，"无法注册应用程序存储库"。

在扫描应用程序存储库时，View Connection Server 调试日志文件中会出现消息。View Connection Server 日志文件位于 View Connection Server 主机上的*驱动器*:`\Documents and Settings\All Users\Application Data\VMware\VDM\logs` 目录中。

无法分配 ThinApp 模板

您无法将 ThinApp 模板分配到桌面或池。

问题

尝试将 ThinApp 模板分配到桌面或池时，View Administrator 返回一个分配错误。

原因

这可能是因为 ThinApp 模板包含一个已分配到桌面或池的应用程序，也可能是因为 ThinApp 模板之前已通过其他安装类型分配到桌面或池。

解决方案

如果该模板中包含一个已分配到桌面或池的 ThinApp 应用程序，则需要创建一个不包含该应用程序的新模板，或者编辑现有模板移除该应用程序。将新的或修改后的模板分配到桌面或池。

要更改 ThinApp 应用程序的安装类型，您必须从桌面或池移除现有应用程序分配。卸载 ThinApp 应用程序之后，可通过其他安装类型将其分配到桌面或池。

ThinApp 应用程序未安装

View Administrator 无法安装 ThinApp 应用程序。

问题

ThinApp 应用程序的安装状态显示为 [Pending Install（正在等待安装）] 或 [Install Error（安装错误）]。

原因

此问题的常见原因包括：

- 桌面上没有足够的磁盘空间来安装 ThinApp 应用程序。
- View Connection Server 主机与桌面之间，或 View Connection Server 主机与应用程序存储库之间的网络连接丢失。

- 无法在网络共享位置访问 ThinApp 应用程序。
- ThinApp 应用程序之前已安装到桌面上，或者桌面上已存在相关目录或文件。

您可以查看 View Agent 和 View Connection Server 日志文件，了解有关问题原因的更多信息。

对于 Windows XP 系统，View Agent 日志文件位于桌面上的*驱动器*:`\Documents and Settings\All Users\Application Data\VMware\VDM\logs` 中；对于 Windows 7 系统，该文件位于*驱动器*:`\ProgramData\VMware\VDM\logs` 中。

View Connection Server 日志文件位于 View Connection Server 主机上的*驱动器*:`\Documents and Settings\All Users\Application Data\VMware\VDM\logs` 目录中。

解决方案

1 在 View Administrator 中，选择 **[Inventory（清单）] > [ThinApp]**。

2 单击 ThinApp 应用程序的名称。

3 在 **[Desktops（桌面）]** 选项卡上，选择桌面并单击 **[Retry Install（重新尝试安装）]** 以重新安装 ThinApp 应用程序。

ThinApp 应用程序未卸载

View Administrator 无法卸载 ThinApp 应用程序。

问题

ThinApp 应用程序的安装状态显示为 [Uninstall Error（卸载错误）]。

原因

此问题的常见原因包括：

- View Administrator 尝试卸载 ThinApp 应用程序时，ThinApp 应用程序正忙。
- View Connection Server 主机与桌面之间失去网络连接。

您可以查看 View Agent 和 View Connection Server 日志文件，了解有关问题原因的更多信息。

对于 Windows XP 系统，View Agent 日志文件位于桌面上的*驱动器*:`\Documents and Settings\All Users\Application Data\VMware\VDM\logs` 中；对于 Windows 7 系统，该文件位于*驱动器*:`\ProgramData\VMware\VDM\logs` 中。

View Connection Server 日志文件位于 View Connection Server 主机上的*驱动器*:`\Documents and Settings\All Users\Application Data\VMware\VDM\logs` 目录中。

解决方案

1 在 View Administrator 中，选择 **[Inventory（清单）] > [ThinApp]**。

2 单击 ThinApp 应用程序的名称。

3 单击 **[Desktops（桌面）]** 选项卡，选择桌面并单击 **[Retry Uninstall（重新尝试卸载）]** 以重试卸载操作。

4 如果卸载操作仍然失败，请手动从该桌面移除 ThinApp 应用程序，然后单击 **[Force Clear Assignment（强制清除分配）]**。

   该命令会在 View Administrator 中清除 ThinApp 应用程序分配，但不会移除该桌面中的任何文件或设置。

   重要事项 请仅在从桌面手动移除 ThinApp 应用程序后使用该命令。

MSI 包无效

View Administrator 报告应用程序存储库中存在无效的 MSI 包。

问题

View Administrator 在扫描操作中报告有一个 MSI 包无效。

原因

此问题的常见原因包括：

- MSI 文件已损坏。
- MSI 文件不是用 ThinApp 创建的。
- MSI 文件是用不受支持的 ThinApp 版本创建的。必须使用 ThinApp 4.6 或更高版本。

解决方案

有关排除 MSI 包问题的信息，请参阅《*ThinApp User's Guide*》（ThinApp 用户指南）。

ThinApp 配置示例

从捕获和打包应用程序到检查安装状态，ThinApp 配置示例将引导您逐步设置典型的 ThinApp 配置。

前提条件

请参阅以下主题全面了解如何在该示例中执行这些步骤。

- 第 180 页，“捕获和存储应用程序包”
- 第 183 页，“将 ThinApp 应用程序分配到桌面和池”

步骤

1. 从 http://www.vmware.com/cn/products/thinapp 下载 ThinApp 软件，并将其安装到干净的计算机上。

   View 支持 ThinApp 4.6 及更高版本。
2. 使用 ThinApp [Setup Capture（安装捕获）] 向导捕获并以 MSI 格式打包应用程序。
3. 在 View Connection Server 主机和 View 桌面均可访问的 Active Directory 域中的某个计算机上创建一个共享文件夹，并在共享文件夹上配置文件和共享权限，为内置 Active Directory 组 "Domain Computers" 授予读访问权限。

   如果您打算将 ThinApp 应用程序分配到域控制器，还必须为内置 Active Directory 组 "Domain Controllers" 授予读访问权限。
4. 将 MSI 包复制到共享文件夹中。
5. 在 View Administrator 中将该共享文件夹注册为应用程序存储库。
6. 在 View Administrator 中，在应用程序存储库中扫描 MSI 包并将选定的 ThinApp 应用程序添加到 View Administrator。
7. 决定将 ThinApp 应用程序分配到桌面还是分配到池。

   如果您对桌面使用了通用命名约定，则可以根据桌面分配快速为使用该命名约定的所有桌面分发应用程序。如果您按部门或用户类型组织池，则可以根据池分配快速为特定部门或用户分发应用程序。

8 在 View Administrator 中，选择要分配到桌面或池的 ThinApp 应用程序并指定安装方法。

选项	操作
Streaming（流式）	在桌面上安装应用程序的快捷方式。该快捷方式指向托管存储库的网络共享位置上的应用程序。用户必须有权访问该网络共享位置才能运行该应用程序。
Full（完整）	在本地文件系统中安装完整的应用程序。

9 在 View Administrator 中，检查 ThinApp 应用程序的安装状态。

管理本地桌面 13

要管理本地模式下使用的桌面，必须对环境进行设置，以便在用户将 View 桌面检出到本地系统时传输数据。您还必须管理其他会产生数据传输的任务（如桌面检入、回滚和备份），并通过策略指定用户可以启动的操作。

本章讨论了以下主题：

在本地模式下使用 View 桌面的优势

利用 View Client with Local Mode，用户可以将 View 桌面检出并下载到本地系统（如笔记本电脑）。管理员可以通过设置备份和连接服务器的频率、对 USB 设备的访问以及检入桌面的权限等策略，管理这些本地 View 桌面。

对于网络连接较差的远程办公室里的员工而言，应用程序在本地 View 桌面上的运行速度比远程桌面更快。这样，用户无论是否连接到网络，都可以使用本地版本的桌面。

如果客户端系统已连接到网络，则检出的桌面将继续与 View Connection Server 进行通信以提供策略更新，并确保本地缓存的身份验证标准为最新标准。默认情况下，系统每隔 5 分钟会尝试一次连接。

View Client with Local Mode 是一个完全受支持的功能，在早期版本中是一个被称为 View Client with Offline Desktop 的试验性功能。

本地模式的 View 桌面与同类远程桌面的运行方式相同，但可以利用本地资源。延迟时间将会消除，性能也会得到改善。用户与其本地 View 桌面断开连接后可以再次登录，而无需连接到 View Connection Server。网络访问恢复后或用户就绪时，检出的虚拟机即可进行备份、回滚或检入。

利用本地资源

本地桌面被检出之后即可利用本地系统上的内存和 CPU 资源。例如，无论为 vCenter Server 中的虚拟机指定何种内存设置，超出主机和客户操作系统所需内存的可用内存都会供主机和本地 View 桌面使用。同样，本地 View 桌面在本地系统上最多可自动使用 2 个可用 CPU，您也可以将本地桌面配置为最多使用 4 个 CPU。

虽然本地桌面可以利用本地资源，但是在 ESX 3.5 主机上创建的 Windows 7 或 Windows Vista View 桌面无法实现 3D 和 Windows Aero 效果。甚至当检出桌面在 Windows 7 或 Windows Vista 主机上进行本地使用时也存在该限制。仅使用 vSphere 4.x 创建的 View 桌面才能呈现 Windows Aero 和 3D 效果。

通过应用本地模式节省数据中心资源

通过要求下载并仅在本地模式下使用 View 桌面，可以降低数据中心在带宽、内存和 CPU 资源方面的成本。员工和承包商有时将此策略称为自备 PC 程序。

检出

当 View 桌面被检出时，vCenter Server 版本的桌面就会被锁定，使其他用户无法进行访问。锁定 View 桌面后，将禁用 vCenter Server 操作，包括启动联机桌面、拍摄快照、编辑虚拟机设置等。但 View 管理员仍然可以监视本地会话和访问 vCenter Server 版本的桌面，以移除访问或回滚桌面。

备份

在备份过程中，vCenter Server 中的 View 桌面会使用所有新数据和配置进行更新，但本地桌面仍保持检出到本地系统中的检出状态，并在 vCenter Server 中保持锁定。

回滚

在回滚过程中，系统会丢弃本地 View 桌面并解锁 vCenter Server 中的相应桌面。以后的客户端连接会定向到 vCenter Server 中的 View 桌面，直到桌面再次被检出。

检入

检入 View 桌面后，本地桌面将上传至 vCenter Server 并解锁相应桌面。以后的客户端连接会定向到 vCenter Server 中的 View 桌面，直到桌面再次被检出。

每个本地系统中的数据均用 AES 进行加密。默认情况下为 128 位加密，不过您可以配置为 256 位加密。桌面的生命周期会通过策略加以控制。如果客户端与 View Connection Server 失去连接，与服务器断开连接的最长时间就是用户访问被拒绝之前可以继续使用桌面的时间。同样，如果移除用户访问，则在缓存过期或客户端通过 View Connection Server 检测到该变更后，客户端系统将无法访问。

View Client with Local Mode 存在以下局限：

- 您必须拥有包含 Local Mode 组件的 View 许可证。
- 执行回滚和检入操作时，最终用户无法访问其本地桌面。
- 只有受 vCenter Server 管理的虚拟机才具有此功能。
- 本地桌面不支持分配用 VMware ThinApp 创建的应用程序包。
- 出于安全性原因，您无法从 View 桌面访问主机 CD-ROM。
- 同样出于安全性原因，您无法在本地系统和 View 桌面之间复制和粘贴文本或系统对象，如文件和文件夹。

本地桌面部署设置概述

要在本地模式下创建和部署 View 桌面，您必须具有所需的许可证、设置 View Transfer Server、使用由 vCenter Server 管理的桌面源，并应用针对本地模式的设置和策略。

创建可在最终用户本地系统上检出使用的桌面时，除了常规设置任务以外，您还必须完成针对本地模式的若干任务。

1 确认您具有 VMware View with Local Mode 组件的许可证。

 在 View Administrator 中，转到 **[View Configuration（View 配置）] > [Product licensing and usage（产品许可和使用情况）]**。

2 确认用于从 View Connection Server 访问 vCenter Server 的用户帐户具有所需的管理员特权。

 要查看正在使用哪个用户帐户，请在 View Administrator 中转至 **[View Configuration（View 配置）] > [Servers（服务器）]**，选择 vCenter Server，然后单击 **[Edit（编辑）]**。

 要查看 vCenter Server operations 操作所需特权的列表，请参阅《*VMware View 安装指南*》中有关配置 vCenter Server 用户帐户的章节。

3 在虚拟机中安装 View Transfer Server，并将该服务器添加到 View Connection Server 配置中。

 在 View Administrator 中，转到 **[View Configuration（View 配置）] > [Servers（服务器）]**。

4 如果您打算使用 View Composer 链接克隆桌面，请配置一个 Transfer Server 存储库。

 在 View Administrator 中，转到 **[View Configuration（View 配置）] > [Transfer Server Repository（Transfer Server 存储库）]**。

5 如果您计划创建一个手动池，请确认该桌面源是一个由 vCenter Server 管理的虚拟机。

6 在 vCenter Server 中创建虚拟机以用作桌面源。

 如果您创建一个比本地客户端系统具有更多虚拟内存和处理器的虚拟机，则该桌面的本地版本将无法开启，并且会显示一条错误消息。

7 如果您计划使用链接克隆桌面，请将桌面的 View Composer 基础映像作为程序包发布在 Transfer Server 存储库中。

 您可以在创建池时或之后发布基础映像。

8 确认已将桌面池的 **[Local Mode（本地模式）]** 策略设置为 **[Allow（允许）]**。

 在 View Administrator 中，转到该池对应的 **[Policies（策略）]** 选项卡。

9 如果您希望桌面仅在本地模式下运行，以使用户必须始终检出桌面，则需要将 **[Remote Mode（远程模式）]** 策略设置为 **[Deny（拒绝）]**。

 在 View Administrator 中，转到该池对应的 **[Policies（策略）]** 选项卡。

10 引导最终用户在他们的本地系统上安装 View Client with Local Mode。

重要事项 另外，在计划部署本地桌面时请注意以下几个方面：

- 创建自动池时，使用专用分配并且仅为专门用于本地模式的桌面创建池。专门用于本地模式的虚拟机可放置在比专门用于支持大量远程 View 桌面的存储的 IOPS 低的数据存储中。同时，由于不支持将 ThinApp 包分配到本地桌面，因此最好的做法就是将 ThinApp 包分配到不含任何本地桌面的池中。
- 如果将桌面配置为使用 RSA 身份验证，则在最终用户与 View Connection Server 建立网络连接的情况下，系统会提示他们提供 RSA 令牌，在未建立网络连接的情况下则不会提示。

将桌面设置为仅在本地模式下运行

通过要求下载并仅在本地模式下使用 View 桌面，可以降低数据中心在带宽、内存和 CPU 资源方面的成本。

如果 View 桌面配置为仅在本地模式下运行，那么最终用户在 View Client 中选择桌面时，就需要下载和检出该桌面。连接桌面和检入桌面的选项对最终用户将不可用。

前提条件

- 确认 View 桌面符合在本地模式下运行的所有要求。

  请参阅第 199 页，“本地桌面部署设置概述”。

- 确保您熟悉针对本地模式的策略和设置。

  请参阅第 212 页，“管理数据传输”。

步骤

1 在 View Administrator 中，查看相应级别的策略。

选项	操作
所有桌面和池	选择 **[Policies（策略）]** > **[Global Policies（全局策略）]** > **[View Policies（View 策略）]** 面板，然后单击 **[Edit Policies（编辑策略）]**。
单个池	选择 **[Inventory（清单）]** > **[Pools（池）]** > ***特定池***。在 **[Policies（策略）]** 选项卡的 **[View Policies（View 策略）]** 窗格中，单击 **[Edit Policies（编辑策略）]**。
单个用户	选择 **[Inventory（清单）]** > **[Pools（池）]** > ***特定池***，然后在 **[Policies（策略）]** 选项卡上单击 **[User Overrides（用户覆盖）]**。

2 将 **[Remote Mode（远程模式）]** View 策略设置为 **[Deny（拒绝）]**。

选项	操作
所有桌面和池或单个池	在 [Edit View Policies（编辑 View 策略）] 对话框中，将 **[Remote Mode（远程模式）]** 设置为 **[Deny（拒绝）]**，然后单击 **[OK（确定）]**。
单个用户	完成 [Add User（添加用户）] 向导以指定用户并将 **[Remote Mode（远程模式）]** 设置为 **[Deny（拒绝）]**。

此时需要下载和检出桌面。

下一步

如果您要阻止最终用户再次检入桌面，请将 **[User-initiated check in（用户启动的检入）]** 策略设置为 **[Deny（拒绝）]**。

如果您要阻止最终用户回滚桌面，请将 **[User-initiated check in（用户启动的回滚）]** 策略设置为 **[Deny（拒绝）]**。

首次检出本地模式桌面

最终用户首次检出 View 桌面在本地模式中使用时，检出和下载过程涉及若干阶段，而且要比后续检出操作花费的时间多。

当最终用户通过 View Client 登录并获得显示一个或多个桌面的列表之后，该用户即可以连接到桌面并将其检出，或是在不先进行远程连接的情况下检出桌面。

重要事项 如果您在登录时使用了 **[Log in as current user（作为当前用户登录）]** 功能，则无法检出桌面。您必须关闭 View Client，将其重新启动并取消选中 **[Log in as current user（作为当前用户登录）]** 复选框。

如果最终用户连接到桌面并将其检出，则该用户会从远程桌面注销，数据中心的虚拟机会被锁定，一个副本虚拟机会被下载至最终用户。

下载完成后，当最终用户首次启动本地桌面时，一些驱动程序将被安装到本地桌面上。安装哪些驱动程序取决于 View 桌面操作系统和本地计算机硬件及操作系统。在安装驱动程序的过程中，View 桌面的性能将受到影响，尤其是在 View 桌面运行 Windows XP 操作系统时。

安装驱动程序后，系统会提示最终用户重新启动本地桌面。

注意 有时，如果在客户操作系统正启动或正关闭时单击 View 桌面窗口，指针会保留在该窗口内。启动完成并且 VMware Tools 运行之后，指针将被释放。如果指针固定在桌面窗口中，可以按 Ctrl+Alt 将其释放。

本地 View 桌面使用的 RAM 容量和 CPU 数量取决于本地计算机的计算能力。View 桌面使用 NAT 共享本地计算机的 IP 和 MAC 地址。有关详细信息，请参阅第 219 页，“配置终端的资源使用情况”。

部署本地桌面的最佳实践

最佳实践建议可以解决有关影响本地模式部署的内存、处理能力和各组件数量的问题。

针对大多数部署的一般建议

虚拟机配置

在本地模式下运行的桌面会根据客户端计算机提供的内存容量自动调整内存使用量和处理能力。由于这种功能，您在 vCenter Server 中创建虚拟机时可以配置客户操作系统所需的最小 RAM 容量和虚拟 CPU 数量。

View Transfer Server

View Transfer Server 的某些功能会占用大量 CPU 资源。如果您打算使用 SSL 进行检出和检入桌面等本地模式操作或将数据复制回数据中心，驻留 Transfer Server 的虚拟机可能需要一个额外的虚拟 CPU。如果您对复制操作开启压缩，您可能还需要更多的处理能力。有关内存和处理器的最低要求，请参阅*《View 安装指南》*中有关 View Transfer Server 的系统要求的主题。

在确定添加到 View Connection Server 上的 View Transfer Server 实例数量时，请确定高可用性是否为重点考虑因素。如果是，请至少添加两个实例。如果其中一个 Transfer Server 出现故障，View Connection Server 会自动向另一个发送请求。

计算所需的 Transfer Server 实例数量时，还要考虑可能会有多少个最终用户同时复制数据或者检出或检入桌面。每个 Transfer Server 实例可以容纳 60 个并发磁盘操作，然而网络带宽可能在数量较少时就会达到饱和。VMware 通过每秒 1 GB 的网络连接测试了 20 个并发磁盘操作，如 20 个客户端同时下载一个本地桌面。

Transfer Server 存储库

View Composer 链接克隆桌面的基础映像保存在某个网络共享位置的 Transfer Server 存储库中。网络存储磁盘运行速度越快，性能就越好。

池设置

使用 View Composer 创建链接克隆桌面池。使用 [Create Pool（创建池）] 向导时，选择专用分配并且仅为专门用于本地模式的桌面创建池。本地模式虚拟机可放置在比专门用于支持大量远程 View 桌面的存储的 IOPS 低的数据存储中。

数据复制

确定最终用户是否需要复制操作系统磁盘数据，如自定义规范中包含的数据。如果不需要，请设置仅复制永久磁盘的策略。

如果您要设置自动复制间隔，可以使用默认的 12 小时或者将间隔设置得更长些。

不要开启重复数据删除或压缩，除非您发现由于网络连接缓慢而引起的问题。重复数据删除和压缩功能虽然可减少所需的网络带宽，但会增加最终用户计算机或 Transfer Server 所需的处理能力。

利用最少的资本支出进行小型部署

如果您在每台服务器上增加虚拟机的数量，您就可以减少部署所需的 ESX 服务器的数量。如果大多数虚拟机没有同时开机，那么一台 ESX 4.1 服务器最多可以托管 500 个虚拟机。

请按照下面的建议减少每个虚拟机所需的带宽量和 I/O 操作，并将 ESX 服务器上的虚拟机数量最大化。

- 设置 View 策略以便最终用户只能在本地模式下使用 View 桌面。进行该设置时，数据中心的虚拟机将保持锁定和关机状态。
- 设置本地模式策略，使最终用户无法启动桌面检入、回滚或复制操作。
- 不要设置自动复制间隔。
- 配置 View Connection Server 设置，使重复数据删除和压缩功能无法用于本地模式操作。这些设置可能仅在以下情况下有用：在网速缓慢的情况下复制本地桌面数据时，最终用户注意到客户端计算机性能下降。
- 配置 View Connection Server 设置，使 SSL 无法用于本地模式操作或部署。
- 使用 View Composer 创建链接克隆桌面，但不使用重构功能。而是使用传统的软件更新机制，将修补程序和更新直接部署到最终用户计算机上的本地桌面。
- 如果 View Connection Server 的性能受本地桌面数量的影响，请将检测信号时间间隔设置得更长些。默认值是 5 分钟。

管理 View Transfer Server

View Transfer Server 是 View 组件，支持本地桌面的数据传输操作。

了解 View Transfer Server

View Transfer Server 管理并简化数据中心与本地桌面之间的数据传输。必须安装 View Transfer Server 才能支持运行 View Client with Local Mode 的桌面。

View Transfer Server 在若干情况下会在远程桌面与本地桌面之间发送数据。

- 当用户检入或检出桌面时，View Manager 将对该操作进行授权和管理。View Transfer Server 会在数据中心与本地桌面之间传输文件。
- View Transfer Server 会将用户做出的更改复制到数据中心，以使本地桌面与数据中心中对应的远程桌面同步。

  复制操作将以您在本地模式策略中指定的时间间隔进行。您也可以在 View Administrator 中启动复制。您可以设置策略，使用户能够从他们的本地桌面启动复制。
- View Transfer Server 从数据中心向本地客户端分发一般系统数据。View Transfer Server 将 View Composer 基础映像从 Transfer Server 存储库下载到本地桌面。
- 如果本地计算机损坏或丢失，那么可以恢复复制到数据中心的数据。

网络中断或是从 View Manager 移除 View Transfer Server 这样的事件会中断正在进行的数据传输。当这些组件再次运行时，View Transfer Server 会恢复暂停的传输。

将 View Transfer Server 添加到 View Manager 中

View Transfer Server 可与 View Connection Server 协作，在本地桌面与数据中心之间传输文件和数据。但您必须将 View Transfer Server 添加到 View Manager 部署中才能执行这些任务。

您可以将多个 View Transfer Server 实例添加到 View Manager 中。这些 View Transfer Server 实例可访问一个公用的 Transfer Server 存储库。它们共享由一个 View Connection Server 实例或副本 View Connection Server 实例组管理的本地桌面的传输负载。

注意 当 View Transfer Server 被添加到 View Manager 时，它的 Distributed Resource Scheduler (DRS) 自动化策略会设置为 [Manual（手动）]，该设置可有效禁用 DRS。

前提条件

- 确认 View Transfer Server 已安装在 Windows Server 虚拟机上。
- 确认 vCenter Server 已添加到 View Manager 中。View Administrator 中的 **[View Configuration（View 配置）] > [Servers（服务器）]** 页面显示了添加至 View Manager 的 vCenter Server 实例。

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 在 [Transfer Server] 面板中，单击 **[Add（添加）]**。

3 在 [Add Transfer Server（添加 Transfer Server）] 向导中，选择管理 View Transfer Server 虚拟机的 vCenter Server 实例，并单击 **[Next（下一步）]**。

4 选择安装 View Transfer Server 的虚拟机，然后单击 **[Finish（完成）]**。

   View Connection Server 将关闭该虚拟机，为其重新配置四个 SCSI 控制器，并重新启动该虚拟机。多个 SCSI 控制器增加了 View Transfer Server 可以同时执行的磁盘传输量。

在 View Administrator 中，View Transfer Server 实例显示在 [Transfer Server] 面板中。如果未配置 Transfer Server 存储库，View Transfer Server 的状态将从 **[Pending（正在等待处理）]** 变为 **[Missing Transfer Server repository（缺少 Transfer Server 存储库）]**。如果配置了 Transfer Server 存储库，其状态将从 **[Pending（正在等待处理）]** 变为 **[Initializing Transfer Server repository（正在初始化 Transfer Server 存储库）]**，最后变为 **[Ready（就绪）]**。

此过程可能需要几分钟时间。您可以单击 View Administrator 中的刷新按钮查看当前状态。

当 View Transfer Server 实例添加至 View Manager 后，View Transfer Server 虚拟机上的 Apache2.2 服务将启动。



小心 如果您的 View Transfer Server 虚拟机版本低于硬件版本 7，将 View Transfer Server 添加至 View Manager 后，您必须在 View Transfer Server 虚拟机上配置静态 IP 地址。

在 View Transfer Server 虚拟机中添加了多个 SCSI 控制器后，Windows 会移除静态 IP 地址，并重新配置虚拟机以使用 DHCP。虚拟机重启后，您必须在虚拟机中重新输入静态 IP 地址。

从 View Manager 中移除 View Transfer Server

从 View Manager 中移除所有 View Transfer Server 实例后，您无法对本地桌面执行检出、检入和数据复制操作。

当您移除正在执行传输操作的 View Transfer Server 实例时，活动传输操作将暂停。本地桌面会话会将传输状态显示为暂停。

例如，如果您在检出桌面时移除 View Transfer Server，检出操作就会暂停。用户可从客户端计算机恢复暂停的传输操作。

注意 您必须在执行以下操作之前将 View Transfer Server 实例从 View Manager 中移除：

- 卸载或升级 View Transfer Server 实例
- 在 vCenter Server 的 View Transfer Server 虚拟机上执行维护操作

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 选择一个 View Transfer Server 实例。

3 单击 **[Remove（移除）]**。

4 如果当前正在进行传输，选择取消当前传输，或取消此次任务并保留 View Transfer Server。

5 单击 **[OK（确定）]**。

当 View Transfer Server 实例从 View Manager 中移除后，其 DRS 自动化策略将被重置为 View Transfer Server 添加到 View Manager 之前的值。

使用维护模式挂起本地桌面的数据传输

当您将 View Transfer Server 实例置于维护模式时，该 View Transfer Server 实例上本地桌面的当前数据传输会被挂起，后续的数据传输也会被阻止。当您将 View Transfer Server 实例退出维护模式后，挂起的传输可从客户端恢复，今后的数据传输也可以正常进行。

当所有 View Transfer Server 实例处于维护模式时，您可以迁移 Transfer Server 存储库。请参阅第 210 页，“将 Transfer Server 存储库迁移到新位置”。

当 View Transfer Server 实例被添加到 View Manager 并处于活动模式时，其 DRS 自动化策略会设置为 [Manual（手动）]，该设置可禁用 DRS。要将 View Transfer Server 实例迁移到其他 ESX 主机或数据存储，请在开始迁移前将该实例置于维护模式。

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 选择一个 View Transfer Server 实例。

3 单击 **[Enter Maintenance Mode（进入维护模式）]**。

4 如果传输正处于活动状态，在将该 View Transfer Server 置于维护模式之前，需要选择是取消活动传输还是等待活动传输完成。

   如果取消活动传输，View Transfer Server 会立即进入维护模式。

   如果您允许活动传输完成，View Transfer Server 会进入 **[Pending（正在等待处理）]** 状态。当传输完成时，它会进入维护模式。

5 单击 **[OK（确定）]**。

下一步

当您准备将 View Transfer Server 退出维护模式后，请选择 View Transfer Server 实例并单击 **[Exit Maintenance Mode（退出维护模式）]**。挂起的传输将会恢复，您可以开始新的数据传输。

提高 Windows Server 2003 上的 WAN 传输性能

在网络延迟较高的 WAN 环境中，您可以通过增加 TCP 发送和接收窗口的大小来提高传输性能。

当 View Transfer Server 安装在 Windows Server 2008 上时，TCP 发送和接收窗口的大小会默认增加到 640 KB。您不必重新配置这些值。

当 View Transfer Server 安装在 Windows Server 2003 上时，您必须手动设置注册表项以将 TCP 发送和接收窗口的大小增加到 640 KB。

前提条件

确认 View Transfer Server 安装在 Windows Server 2003 操作系统上。

步骤

1 在安装有 View Transfer Server 的 Windows Server 2003 计算机上启动 Windows 注册表编辑器。

2 新建 **[DefaultSendWindow]** 和 **[DefaultReceiveWindow]** 注册表项并将其添加到 **[HKEY_LOCAL_MACHINE] > [System] > [CurrentControlSet] > [Services] > [AFD] > [Parameters]**。

3 将 **[DefaultSendWindow]** 和 **[DefaultReceiveWindow]** 项的值设置为 `655360`。

您必须键入一个正整数。按字节配置这些值。项类型为 **REG_DWORD**。

4 重新启动 View Transfer Server。

View Transfer Server 状态

View Transfer Server 有多种运行状态和可用性状态。在 View Administrator 中，您可以在 **[View Configuration（View 配置）] > [Servers（服务器）]** 页面上的 [Transfer Servers（传输服务器）] 窗格中跟踪 View Transfer Server 的状态。

表 13–1 正常操作过程中的 View Transfer Server 状态

状态	描述
Ready（就绪）	View Transfer Server 和 Transfer Server 存储库已配置且可以正常运行。
Pending（正在等待处理）	View Transfer Server 正被添加到 View Manager 或正在退出 [Maintenance（维护）] 模式。View Connection Server 正在与 View Transfer Server 建立连接。 建立连接后，View Transfer Server 将转为 [Ready（就绪）] 等运行状态。
Maintenance mode pending（维护模式正在等待处理）	View Transfer Server 在等待活动传输和程序包发布完成时会进入 [Maintenance（维护）] 模式。
Maintenance mode（维护模式）	活动的数据传输被挂起。用户无法启动新传输。正在等待处理的计划传输无法进行。View Transfer Server 无法将程序包发布到 Transfer Server 存储库。
Initializing Transfer Server repository（正在初始化 Transfer Server 存储库）	View Transfer Server 正在初始化 Transfer Server 存储库。 如果 View Transfer Server 在初始化 Transfer Server 存储库时遇到问题，该状态会变为错误状态。要解决该问题，请参见有关显示的错误状态的故障排除提示。

View Transfer Server 变得不可用或无法正常运行时会进入错误状态。要解决问题，请阅读有关显示的错误状态的故障排除提示。请参阅第 230 页，“排除 View Transfer Server 和本地桌面操作问题”。

表 13–2 View Transfer Server 错误状态

状态	描述
Bad Transfer Server repository（无效的 Transfer Server 存储库）	View Transfer Server 需要连接的 Transfer Server 存储库与当前在 View Connection Server 中配置的 Transfer Server 存储库不同。
Repository connection error（存储库连接错误）	View Transfer Server 无法连接到配置的 Transfer Server 存储库。

表 13–2 View Transfer Server 错误状态 （续）

状态	描述
Bad health check（无效的运行状况检查）	View Transfer Server 无法执行 View Manager 运行状况检查。View Transfer Server 不可用或无法正常运行。
Missing Transfer Server repository（缺少 Transfer Server 存储库）	View Connection Server 中未配置 Transfer Server 存储库。
Transfer Server repository conflict（Transfer Server 存储库冲突）	多个 View Transfer Server 实例被配置为连接到不同的 Transfer Server 存储库。 如果同时将多个 View Transfer Server 实例添加到了 View Manager 中，并为每个实例配置不同的 Transfer Server 存储库，就可能出现此状态。
Web Server down（Web 服务器关闭）	支持 Transfer Server 存储库的 Apache2.2 服务未运行。

管理 Transfer Server 存储库

View Transfer Server 使用 Transfer Server 存储库来存储下载到本地桌面的 View Composer 基础映像。要检出链接克隆桌面在本地模式运行，必须要配置 Transfer Server 存储库。

使用 Transfer Server 存储库下载系统映像

为支持以本地模式运行的链接克隆桌面，Transfer Server 存储库会将 View Composer 基础映像存储在可访问的数据存储中。View Manager 和 View Transfer Server 可从 Transfer Server 存储库部署和更新链接克隆本地桌面。

您必须先将链接克隆桌面的基础映像发布到 Transfer Server 存储库，用户才能检出该桌面在本地模式下运行。

当您将映像文件发布到 Transfer Server 存储库时，View Transfer Server 会将文件打包加密存储。View Transfer Server 可以压缩程序包，从而简化下载到本地桌面的过程。

当用户首次检出链接克隆桌面时，View Transfer Server 会执行两个操作：

- 将基础映像从 Transfer Server 存储库下载到本地计算机。
- 将远程链接克隆桌面从数据中心下载到本地计算机上。桌面由链接克隆的操作系统磁盘和 View Composer 永久磁盘组成。

当您在数据中心运行链接克隆桌面时，多个链接克隆可以共同访问一个基础映像。当您在本地模式下运行链接克隆桌面时，必须有一份基础映像副本与链接克隆桌面一起驻留在本地计算机上。

如果基础映像保持不变，就只会下载一次。当用户再次检入和检出桌面时，View Transfer Server 会下载链接克隆的操作系统磁盘和 View Composer 永久磁盘，而不会下载基础映像。

如果基础映像已经过重构，那么用户下次检出桌面时，View Transfer Server 会将更新的基础映像从 Transfer Server 存储库下载到本地计算机上。有关详细信息，请参阅第 151 页，“重构能够以本地模式运行的链接克隆桌面”。

重要事项 从基础映像创建的链接克隆桌面必须先检入数据中心，您才可以对其进行重构。

确定 View Composer 基础映像的大小

Transfer Server 存储库必须足够大才能为本地模式中使用的所有链接克隆桌面存储 View Composer 基础映像。要确保 Transfer Server 存储库可以容纳特定的基础映像，您可以确定基础映像的适当大小。

基础映像的大小可以为几千兆字节。

基础映像的最大大小为父虚拟机中部署的硬盘大小之和。实际的基础映像大小可能小于最大值。

前提条件

确认您创建了一个用于创建链接克隆桌面池的父虚拟机。

步骤

1 在 vSphere Client 中，选择父虚拟机。

2 单击 **[Edit Settings（编辑设置）]**。

3 在 **[Hardware（硬件）]** 选项卡中，选择第一个配置的硬盘。

   例如，选择 **[Hard Disk 1（硬盘 1）]**。

4 在 [Disk Provisioning（磁盘部署）] 窗格中，查看 [Provisioned Size（部署的大小）]。

5 如果虚拟机有多个硬盘，则为每个附加硬盘重复步骤 3 和步骤 4。

6 增加为硬盘的部署的容量。

配置 Transfer Server 存储库

Transfer Server 存储库存储了本地模式下运行的链接克隆桌面的 View Composer 基础映像。要使 View Transfer Server 能够访问 Transfer Server 存储库，您必须在 View Manager 中配置该存储库。如果您不在本地模式下使用 View Composer 链接克隆，则无需配置 Transfer Server 存储库。

如果在您配置 Transfer Server 存储库之前已在 View Manager 中配置了 View Transfer Server，View Transfer Server 会在配置过程中验证 Transfer Server 存储库的位置。

如果打算将多个 View Transfer Server 实例添加到该 View Manager 部署中，则应当在一个网络共享位置配置 Transfer Server 存储库。其他 View Transfer Server 实例无法访问在 View Transfer Server 实例的本地驱动器上配置的 Transfer Server 存储库。

如果要在网络共享位置配置远程 Transfer Server 存储库，则必须提供具有可访问网络共享位置的凭据的用户 ID。作为最佳实践，为增强访问 Transfer Server 存储库的安全性，请确保仅限 View 管理员才可通过网络访问资源库。

前提条件

- 确认 View Transfer Server 已安装在 Windows Server 虚拟机上。
- 确认 View Transfer Server 已添加到 View Manager 中。请参阅第 203 页，“将 View Transfer Server 添加到 View Manager 中”。

  注意 最佳实践是在配置 Transfer Server 存储库前将 View Transfer Server 添加到 View Manager，但不是强制要求。

- 确定 Transfer Server 存储库必须达到的大小，以存储 View Composer 基础映像。基础映像的大小可以为几千兆字节。要确认特定基础映像的大小，请参阅第 206 页，“确定 View Composer 基础映像的大小”。

步骤

1 为 Transfer Server 存储库配置路径和文件夹。

Transfer Server 存储库可以位于本地驱动器或网络共享位置上。

选项	操作
Local Transfer Server repository（本地 Transfer Server 存储库）	在安装了 View Transfer Server 的虚拟机上，为 Transfer Server 存储库创建路径和文件夹。 例如：`C:\TransferRepository\`
Remote Transfer Server repository（远程 Transfer Server 存储库）	为网络共享位置配置 UNC 路径。 例如：`\\server.domain.com\TransferRepository\` 您添加到 View Manager 部署中的所有 View Transfer Server 实例都必须能通过网络访问该共享驱动器。

2 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

3 将所有 View Transfer Server 实例置于维护模式下。

a 在 [Transfer Server] 面板中，选择一个 View Transfer Server 实例。

b 单击 **[Enter Maintenance Mode（进入维护模式）]**，然后单击 **[OK（确定）]**。

View Transfer Server 的状态将变为 **[Maintenance mode（维护模式）]**。

c 对每个实例重复 步骤 3a 和 步骤 3b。

当所有 View Transfer Server 实例均处于维护模式时，当前的传输操作将停止。

4 在 [Transfer Server] 面板中，单击 Transfer Server 存储库旁边的 **[None Configured（未配置）]**。

5 在 Transfer Server 存储库页面的 [General（常规）] 面板中，单击 **[Edit（编辑）]**。

6 键入 Transfer Server 存储库的位置及其他信息。

选项	描述
网络共享位置	■ **Path（路径）**：键入您配置的 UNC 路径。 ■ **Username（用户名）**：键入具有访问网络共享位置的凭据的管理员用户 ID。 ■ **Password（密码）**：键入管理员密码。 ■ **Domain（域）**：以 NetBIOS 格式键入网络共享位置的域名。不要使用 `.com` 后缀。
本地文件系统	键入您在本地 View Transfer Server 虚拟机上配置的路径。

7 单击 **[OK（确定）]**。

如果存储库网络路径或本地驱动不正确，则 [Edit Transfer Server Repository（编辑 Transfer Server 存储库）] 对话框将会显示错误消息，并且不允许您配置位置。您必须键入一个有效位置。

8 在 **[View Configuration（View 配置）] > [Servers（服务器）]** 页面中，选择该 View Transfer Server 实例，然后单击 **[Exit Maintenance Mode（退出维护模式）]**。

View Transfer Server 的状态将变为 **[Ready（就绪）]**。

在 Transfer Server 存储库中发布程序包文件

您必须先将链接克隆桌面的 View Composer 基础映像作为程序包发布到 Transfer Server 存储库中，用户才能检出该桌面。

用户检出某个链接克隆桌面后，View Transfer Server 会将该克隆的基础映像程序包文件从 Transfer Server 存储库下载到本地计算机。

您可以从 View Administrator 的 **[Transfer Server repository（Transfer Server 存储库）]** 页面发布程序包。此外，也可以在创建链接克隆池时发布程序包。创建池后，您还可以使用 **[View Composer] > [Publish(发布)]** 选项，从单独的池页面发布程序包。

前提条件

- 确认在 View Manager 中配置了 View Transfer Server 实例。请参阅第 203 页，“将 View Transfer Server 添加到 View Manager 中”。
- 确认在 View Manager 中配置了 Transfer Server 存储库。请参阅第 207 页，“配置 Transfer Server 存储库”。
- 确认 Transfer Server 存储库的大小足够容纳基础映像（可以是几千兆字节)。在程序包文件被压缩之前，存储库必须具有容纳基础映像所需的空间。请参阅第 206 页，“确定 View Composer 基础映像的大小”。
- 确认已创建了将在本地模式中使用的链接克隆桌面池。

步骤

1. 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Transfer Server Repository（Transfer Server 存储库）]**。
2. 单击 **[Publish（发布）]**。
3. 从列表中选择一个 View Composer 基础映像，然后单击 **[Next（下一步）]**。
4. 单击 **[Finish（完成）]**。

该程序包将显示在 [Transfer Server Repository（Transfer Server 存储库）] 页面的 [Contents（内容）] 窗格中。程序包状态会从 **[Initializing（正在初始化）]** 改为 **[Publishing（正在发布）]**，之后改为 **[Published（已发布）]**。

发布过程需要一定的时间。单击 [Transfer Repository（Transfer 存储库）] 页面上的刷新图标可显示操作完成的百分比。

View Transfer Server 会将发布的 View Composer 基础映像下载到本地桌面。

从 Transfer Server 存储库删除程序包文件

View Transfer Server 将 View Composer 基础映像作为程序包文件存储在 Transfer Server 存储库中。当这些文件过期或不再使用时，您可以将程序包从 Transfer Server 存储库中删除。

即使链接克隆桌面仍然使用发布程序包文件的基础映像，您也可以删除该程序包文件。删除程序包文件之后，这些桌面将无法检出。

前提条件

- 确认已在 View Manager 中配置 View Transfer Server。请参阅第 203 页，“将 View Transfer Server 添加到 View Manager 中”。
- 确认已配置 Transfer Server 存储库。请参阅第 207 页，“配置 Transfer Server 存储库”。

步骤

1. 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Transfer Server Repository（Transfer Server 存储库）]**。
2. 在 [Contents（目录）] 面板中，选择一个程序包。
3. 单击 **[Remove（移除）]**。

   此时会弹出一个对话框，警告您链接克隆桌面是否正在使用发布所选程序包文件的基础映像。您可以取消程序包移除操作或继续。
4. 单击 **[OK（确定）]**。

程序包将进入 **[Pending Delete（待删除）]** 状态并被删除。

将 Transfer Server 存储库迁移到新位置

如果当前磁盘驱动器的空间已满，您可以将 Transfer Server 存储库迁移到新位置。

必须先将所有与 View Connection Server 关联的 View Transfer Server 实例都置于维护模式，您才能迁移 Transfer Server 存储库。

如果具有多个 View Transfer Server 实例，应当将 Transfer Server 存储库迁移到网络共享驱动器。其他 View Transfer Server 实例无法访问在 View Transfer Server 实例的本地驱动器上配置的 Transfer Server 存储库。

前提条件

确认已经安装并配置了 View Transfer Server。请参阅第 203 页，“将 View Transfer Server 添加到 View Manager 中”。

步骤

1 配置一个本地或远程目标文件夹，将 Transfer Server 存储库迁移到其中。

选项	操作
Local Transfer Server repository（本地 Transfer Server 存储库）	在安装了 View Transfer Server 的虚拟机上，为 Transfer Server 存储库创建路径和文件夹。 例如：`C:\TransferRepository\`
Remote Transfer Server repository（远程 Transfer Server 存储库）	为网络共享位置配置 UNC 路径。 例如：`\\server.domain.com\TransferRepository\` 您添加到 View Manager 部署中的所有 View Transfer Server 实例都必须能通过网络访问该共享驱动器。

2 将 Transfer Server 存储库根路径手动复制到目标位置。

您必须复制整个根路径，而不仅仅是根路径下的文件包。

3 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

4 将所有 View Transfer Server 实例置于维护模式下。

a 在 [Transfer Server] 面板中，选择一个 View Transfer Server 实例。

b 单击 **[Enter Maintenance Mode（进入维护模式）]**，然后单击 **[OK（确定）]**。

View Transfer Server 的状态将变为 **[Maintenance（维护）]**。

c 对每个实例重复这些步骤。

当所有 View Transfer Server 实例均处于维护模式时，当前的传输操作将停止。

5 在 [Transfer Server] 面板中，单击 Transfer Server 存储库的路径。

例如：`C:\TransferRepository`。

6 在 Transfer Server 存储库页面的 [General（常规）] 面板中，单击 **[Edit（编辑）]**。

7 键入目标 Transfer Server 存储库的位置及其他信息。

选项	描述
Network Share（网络共享位置）	■ **Path（路径）**：键入您配置的 UNC 路径。 ■ **Username（用户名）**：键入具有访问网络共享位置的凭据的管理员用户 ID。 ■ **Password（密码）**：键入该管理员的密码。 ■ **Domain（域）**：以 NetBIOS 格式键入网络共享位置的域名。不要使用 `.com` 后缀。
Local File System（本地文件系统）	键入您在本地 View Transfer Server 虚拟机上配置的路径。

8 单击 **[OK（确定）]**。

9 在 **[View Configuration（View 配置）]** > **[Servers（服务器）]** 页面中，选择每个 View Transfer Server 实例，单击 **[Exit Maintenance Mode（退出维护模式）]**，然后单击 **[OK（确定）]**。

   View Transfer Server 的状态将变为 **[Ready（就绪）]**。

10 （可选）从原来的 Transfer Server 存储库文件夹中手动删除程序包文件。

从损坏的 Transfer Server 存储库文件夹进行恢复

如果配置有 Transfer Server 存储库的网络共享文件夹或本地文件夹损坏，您就必须在一个正常工作的文件夹上重新创建 Transfer Server 存储库。

如果网络共享位置或本地驱动器不可访问，而且您无法访问存储在所配置文件夹中的 Transfer Server 程序包文件，就会发生这种情况。在这种情况下，您无法手动将程序包文件从损坏的文件夹复制到新文件夹。

前提条件

- 熟悉如何配置 Transfer Server 存储库。请参阅第 207 页，“配置 Transfer Server 存储库”。
- 熟悉如何在 View Manager 中移除和添加 View Transfer Server 以及如何将 View Transfer Server 置于维护模式。请参阅第 202 页，“管理 View Transfer Server”。
- 熟悉如何在 Transfer Server 存储库中发布和删除程序包。请参阅第 208 页，“在 Transfer Server 存储库中发布程序包文件”和第 209 页，“从 Transfer Server 存储库删除程序包文件”。

步骤

1 从 View Manager 中移除 View Transfer Server 的所有实例。

   当 View Transfer Server 的所有实例被移除后，View Manager 会删除 Transfer Server 存储库配置，包括路径和相关信息。

2 为网络共享位置或本地驱动器配置新路径和文件夹。

   遵循您在新建 Transfer Server 存储库时采用的操作流程。

3 将 View Transfer Server 实例添加到 View Manager 中。

4 将 View Transfer Server 实例置于维护模式。

5 在 View Manager 中配置 Transfer Server 存储库，指定新的网络共享位置或本地路径。

   View Transfer Server 会验证新的 Transfer Server 存储库路径。每个程序包的状态均为 **[Missing Package（缺少程序包）]**。

6 通过退出维护模式将每个 View Transfer Server 实例返回至 **[Ready（就绪）]** 状态。

7 从 Transfer Server 存储库删除转移的程序包。

8 将程序包重新发布到 Transfer Server 存储库。

   使用原始父虚拟机和快照，将 View Composer 基础映像作为程序包发布到存储库中。

管理数据传输

您可以设置策略来配置复制操作和优化传输操作。此外，还可以在两次计划的复制操作之间发起复制请求。如有必要，您可以回滚桌面以放弃本地检出的版本。

复制操作按次序进行，可保持本地桌面数据的完整性。

每个复制操作都将传输复制启动时为本地桌面拍摄的快照中的数据。因此，每个副本都代表本地桌面的一个不同状态。

当您启动复制，或者复制按计划启动时，其请求将在客户端计算机下次与数据中心通信时开始。View Client with Local Mode 会拍摄快照并启动复制。

View 每次仅维护一个等待处理的复制。

注意 在每个复制的开始和结束阶段，最终用户可能会注意到拍摄或更新本地快照时，桌面性能都会受到几秒钟的影响。

- 设置复制策略第 212 页，

  复制操作通过将用户所做的更改发送到数据中心，使本地桌面与相应的远程桌面同步。您可以设置策略来配置复制频率，允许用户延迟复制并选择要复制的链接克隆磁盘的类型。

- 启动本地桌面复制第 213 页，

  您可以启动复制本地模式下运行的桌面。您的请求会在按计划启动的下一次复制之前启动一次复制操作。如果客户端策略允许，则检出本地桌面的最终用户还可以从 View Client 中启动复制。

- 回滚本地检出的桌面第 214 页，

  如果最终用户丢失了包含本地桌面的笔记本电脑，或者硬盘受损，您可以回滚 View 桌面，以使最终用户能够在另一台计算机上检出桌面。如果客户端策略允许，则检出本地桌面的最终用户还可以从 View Client 中回滚桌面。

- 删除本地桌面第 214 页，

  在回滚本地桌面或卸载 View Client 时，在客户端计算机上组成本地桌面的文件不会被删除或清空。要移除本地桌面，您必须手动删除它的文件。

设置复制策略

复制操作通过将用户所做的更改发送到数据中心，使本地桌面与相应的远程桌面同步。您可以设置策略来配置复制频率，允许用户延迟复制并选择要复制的链接克隆磁盘的类型。

您需要通过设置本地模式策略来配置复制功能。有关说明，请参阅第 125 页，“本地模式策略”。

前提条件

确定是否针对单个桌面池和单个用户来全局设置这些策略。有关详细信息，请参阅第 123 页，“在 View Administrator 中设置策略”。

步骤

- 设置 **[Target replication frequency（目标复制频率）]**。

  此策略可指定启动两次复制之间的时间间隔（以天、小时或分钟为单位）。通过选择 **[No replication（不复制）]**，可以禁止计划的复制。

  [No replication（不复制）] 策略不会禁止显式复制请求。您可以在 View Administrator 中启动复制，如果 **[User initiated replication（用户启动的复制）]** 策略设置为 **[Allow（允许）]**，那么用户可以请求复制。

  如果复制花费的时间比 **[Target replication frequency（目标复制频率）]** 策略中指定的时间间隔长，那么按计划启动的复制将在前一次复制完成后开始。等待处理的复制不会取消前一次复制。

  例如，**[Target replication frequency（目标复制频率）]** 策略可能设置为一天。复制可能会在星期二中午开始。如果客户端计算机断开网络连接，那么复制时间可能超过 24 小时。在星期三中午，View Client with Local Mode 会启动下一复制请求。前一次复制完成后，View Client with Local Mode 会拍摄快照并启动等待处理的复制。

- 设置 **[User deferred replication（用户延迟的复制）]**。

  此策略允许用户暂停正在进行的复制。在延迟期限结束之前，复制不会恢复，也不会开始新的复制。延迟期限为两个小时。

- 设置 **[Disks replicated（复制的磁盘）]**。

  此策略用于确定是仅复制 View Composer 永久磁盘或操作系统磁盘，还是两者都复制。此策略仅影响链接克隆桌面。

  在桌面被检出的情况下可设置此策略。如果您更改策略，所做的更改会在桌面下次被检出时生效。

- 设置 **[User initiated replication（用户启动的复制）]**。

  此策略允许用户从本地桌面请求复制。

启动本地桌面复制

您可以启动复制本地模式下运行的桌面。您的请求会在按计划启动的下一次复制之前启动一次复制操作。如果客户端策略允许，则检出本地桌面的最终用户还可以从 View Client 中启动复制。

如果您在 View Client with Local Mode 已经开始复制数据的情况下启动复制，您请求的复制会在前一次复制完成后开始。等待处理的请求不会中止前一次复制。

步骤

1 在 View Administrator 中，单击 **[Monitoring（监视）] > [Local Sessions（本地会话）]**。

2 选择本地桌面。

3 单击 **[Initiate Replication（启动复制）]**。

4 选择是否在本地桌面与数据中心下次连接时启动复制。

选项	描述
Yes（是）	在下次 View Client 运行并且桌面与数据中心通信时启动复制。
No（否）	取消您的复制请求。 如果您先前请求了复制操作，但尚未启动，则可以选择 **[No（否）]** 取消等待处理的复制请求。

5 单击 **[OK（确定）]**。

复制操作将在下次 View Client 运行并且客户端计算机与数据中心通信时启动。如果正在进行复制操作，您请求的复制将在前一次复制完成后开始。

下一步

如果您因为要在不进行最终用户交互的情况下重新检入桌面而启动复制，可以在复制完成后回滚本地桌面。请参阅第 214 页，“回滚本地检出的桌面”。

回滚本地检出的桌面

如果最终用户丢失了包含本地桌面的笔记本电脑，或者硬盘受损，您可以回滚 View 桌面，以使最终用户能够在另一台计算机上检出桌面。如果客户端策略允许，则检出本地桌面的最终用户还可以从 View Client 中回滚桌面。

如果管理员启动回滚操作，客户端应采取以下操作之一：

- 如果用户登录已检出的桌面，一旦 View Client 接收到通知，会话即会终止。用户将无法再登录检出的桌面。
- 如果用户未登录，则后续连接尝试将被重定向到桌面的联机副本。要继续在本地模式下工作，用户必须立即从服务器中检出桌面。

前提条件

如果管理员希望保留本地桌面中的最新数据，可执行复制操作。请参阅第 213 页，“启动本地桌面复制”。

重要事项 如果要执行复制，必须等到复制完成后再启动回滚操作。回滚操作不排在其他操作之后。要确定复制操作何时完成，请在 View Administrator 中单击 **[Monitoring（监视）] > [Local Sessions（本地会话）]** 并注意上一次复制完成的时间。

步骤

◆ 选择 **[Rollback（回滚）]** 选项。

选项	操作
View Administrator 用户	在 View Administrator 中，选择 **[Monitoring（监视）] > [Local Sessions（本地会话）]**，然后选择所需的桌面，单击 **[Rollback（回滚）]**。
最终用户	如果您是有权访问桌面的用户，请在 View Client 中右键单击可用桌面列表中的桌面，然后选择 **[Rollback（回滚）]**。 仅在客户端桌面策略允许的情况下，**[Rollback（回滚）]** 选项才可用。

检出的桌面版本将被放弃。用户必须再次检出联机版本，才能在本地模式下使用桌面。

下一步

要清除最终用户计算机上的文件，请让最终用户删除此桌面的本地模式目录。请参阅第 214 页，“删除本地桌面”。

有关检出 View 桌面以在本地模式下使用的信息，请参阅 *《View 安装指南》*。

删除本地桌面

在回滚本地桌面或卸载 View Client 时，在客户端计算机上组成本地桌面的文件不会被删除或清空。要移除本地桌面，您必须手动删除它的文件。

前提条件

确认本地桌面不再被检出。如果本地桌面包含尚未复制到位于数据中心的 View 桌面的数据，请要求最终用户检入桌面。如果无法检入桌面，请使用 View Administrator 复制数据。请参阅第 213 页，“启动本地桌面复制”。

步骤

◆ 在客户端计算机上，选择并删除包含组成您要删除的本地桌面的文件的文件夹。

文件夹位于本地桌面检出目录下。下载首个本地桌面时，如果您未单击 **[Options（选项）]** 并更改本地桌面的存储目录，那么它们就存储在默认的检出目录下。

桌面操作系统	默认检出目录
Windows 7 和 Windows Vista 上的默认目录	`C:\Users\`*用户名*`\AppData\Local\VMware\VDM\Local Desktops\`*池显示名称*
Windows XP 上的默认目录	`C:\Documents and Settings\`*用户名*`\Local Settings\Application Data\VMware\VDM\Local Desktops\`*池显示名称*

Windows 7 操作系统中的 `AppData` 目录为隐藏文件夹。您可能需要显示该隐藏文件夹以导航到本地桌面文件。

针对本地桌面操作进行安全和优化配置

您可以为本地桌面操作配置安全加密链路通信和 SSL 加密。此外，还可以优化本地计算机与数据中心之间的数据传输。

这些设置专门针对某一个 View Connection Server 实例。您可能需要在服务于从 Internet 连接的本地桌面用户的实例中启用这些设置，而在不使用本地桌面的内部用户专用的实例中禁用这些设置。

前提条件

- 熟悉针对本地桌面操作的 SSL 和安全加密链路通信设置。请参阅第 216 页，“为本地桌面操作设置安全选项”。
- 熟悉如何使用重复数据删除和压缩功能来优化网络中的数据传输。请参阅第 215 页，“优化本地桌面主机与数据中心之间的数据传输”。

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 在 [View Server] 面板中，选择一个 View Connection Server 实例，然后单击 **[Edit（编辑）]**。

3 针对数据传输和本地桌面操作选择安全和优化设置。

优化本地桌面主机与数据中心之间的数据传输

在驻留本地桌面的客户端计算机与数据中心之间进行数据传输时，您可以减少通过网络发送的数据量。您可以通过重复数据删除和压缩功能来优化数据传输。

表 13-3 显示了用于数据传输的重复数据删除和压缩设置。

传输操作包括检入和检查桌面，从本地桌面向数据中心复制数据，以及将系统映像下载到本地桌面。

通过阅读 View Client with Local Mode 日志，可以确定重复数据删除和压缩对数据传输的影响。请参阅第 218 页，“确定重复数据删除和压缩对数据传输的影响”。

表 13–3 用于数据传输的重复数据删除和压缩设置

设置	描述
Use deduplication for Local Mode operations（为本地模式操作使用重复数据删除）	防止从客户端计算机向数据中心发送冗余数据。重复数据删除应用于从客户端计算机向数据中心的数据传输，包括复制和桌面检入。检出桌面时不会进行重复数据删除。 利用重复数据删除功能，客户端计算机会检测完全相同的数据块，并发送一份原始数据块参考，而不会再次发送整个数据块。 在网速较低的情况下，重复数据删除功能尤其适用，因为它可以节省网络带宽。然而，重复数据删除功能在查找相同数据块时会增加客户端计算机上的 CPU 工作负载，在从磁盘读取复制块时会增加 View Transfer Server 上的 I/O 工作负载。如果网速较高，禁用重复数据删除功能可能有助于提高效率。 默认设置为不使用重复数据删除功能。
Use compression for Local Mode operations（为本地模式操作使用压缩功能）	在通过网络发送系统映像和桌面文件之前先进行压缩。 与重复数据删除功能相似，压缩功能可在网速较低的情况下节省带宽，提高传输速度。但是，View Transfer Server 需要使用更多计算资源来压缩文件。在决定是否使用压缩功能时，您必须权衡网络性能与服务器计算成本这两方面的因素。 默认设置为不使用压缩功能。

为本地桌面操作设置安全选项

通过在驻留本地桌面的客户端计算机与数据中心之间使用 SSL 加密连接和安全加密链路连接，您可以设置传输操作的安全级别。

表 13–4 显示了针对本地桌面操作的安全设置。

不使用 SSL 或安全加密链路连接可提高数据传输速度，但是会降低数据通信的安全性。

SSL 设置不会影响客户端计算机上的本地数据，这些数据始终是加密的。

表 13–4 为本地桌面操作使用安全加密链路连接和 SSL

设置	描述
Use secure tunnel connection for Local Mode operations（为本地模式操作使用安全加密链路连接）	本地桌面使用安全加密链路进行通信。网络流量将通过 View Connection Server 或安全服务器（如已配置）传送。 如果您不使用该设置，数据传输将直接在本地桌面和数据中心内相应的远程桌面间进行。 默认设置是使用安全加密链路连接而非直接连接。
Use SSL for Local Mode operations（为本地模式操作使用 SSL）	客户端计算机与数据中心之间的通信和数据传输使用 SSL 加密。这些操作包括：检入和检出桌面、从客户端计算机向数据中心复制数据。这些操作涉及客户端计算机与 View Transfer Server 之间的连接。 默认设置为不使用 SSL。
Use SSL when provisioning desktops in Local Mode（部署本地模式桌面时使用 SSL）	将 View Composer 基础映像文件从 Transfer Server 存储库传输到客户端计算机时使用 SSL 加密。这些操作涉及客户端计算机与 View Transfer Server 之间的连接。 默认设置为不使用 SSL。

更改本地桌面加密密钥密码以生成新密钥

默认情况下，当用户检入和检出本地桌面时，View Connection Server 使用 AES-128 对虚拟磁盘 (`.vmdk`) 文件进行加密。如果您想使用更强的加密计算，可在 View Connection Server 主机的 View LDAP 中编辑一个全局属性，将加密密钥密码更改为 AES-192 或 AES-256。

更改本地桌面的加密密钥密码后，新密码将用于生成新密钥（如在本地桌面被首次检出时生成）。之前生成的密钥不会更改。要更改现有本地桌面的加密密钥密码，请参阅第 217 页，“更改现有本地桌面的加密密钥密码”。

您可以使用“ADSI 编辑”实用程序修改 View LDAP。“ADSI 编辑”实用程序随 View Connection Server 一起安装。在 View Connection Server 实例上更改 View LDAP 时，所作更改会传播给所有副本 View Connection Server 实例。

前提条件

请参阅 Microsoft TechNet 网站，了解如何在您的 Windows 操作系统版本上使用“ADSI 编辑”实用程序。

步骤

1 在您的 View Connection Server 主机上启动“ADSI 编辑”实用程序。

2 选择或连接到 **[DC=vdi, DC=vmware, DC=int]**。

3 在对象 **[CN=Common, OU=Global, OU=Properties]** 上，将 **[pae-OVDIKeyCipher]** 属性设置为新的加密密钥密码值。

   您可以将加密密钥密码值设置为 **`AES-128`**、**`AES-192`** 或 **`AES-256`**。默认值为 **`AES-128`**。

更改现有本地桌面的加密密钥密码

要更改现有本地桌面的加密密钥密码，您需要在 View Connection Server 主机的 View LDAP 中编辑本地桌面的 **pae-VM** 记录。

您可以使用“ADSI 编辑”实用程序修改 View LDAP。“ADSI 编辑”实用程序随 View Connection Server 一起安装。在 View Connection Server 实例上更改 View LDAP 时，所作更改会传播给所有副本 View Connection Server 实例。

前提条件

- 更改本地桌面的加密密钥密码。请参阅第 217 页，“更改本地桌面加密密钥密码以生成新密钥”。
- 请参阅 Microsoft TechNet 网站，了解如何在您的 Windows 操作系统版本上使用“ADSI 编辑”实用程序。

步骤

1 如果本地桌面已被检出，请将其检入并移除所有现有的本地文件。

2 在您的 View Connection Server 主机上启动“ADSI 编辑”实用程序。

3 选择或连接到 **[DC=vdi, DC=vmware, DC=int]**。

4 在本地桌面的 **[pae-VM]** 记录中，清除 **[pae−mVDIOfflineAuthKey]**、**[pae−mVDIOfflineDataKey]** 和 **[pae-mVDIOfflineObfuscationKey]** 属性的值。

5 检出本地桌面。

View Connection Server 会为本地桌面生成新的密钥。新密钥中具有新的加密密钥密码值。

确定重复数据删除和压缩对数据传输的影响

您可以确定在数据传输过程中重复数据删除和压缩在多大程度上降低了通过网络发送的数据量。通过阅读客户端计算机上的 View Client with Local Mode 日志，您可以获取数据传输的大小。

在检入或复制过程中，如果没有进行优化，本地桌面就会显示将被传输到数据中心的远程桌面的数据量。该数据量不能反映通过网络发送的实际数据。无论是否启用重复数据删除和压缩，都会显示相同的数字。

当同时启用这两个功能时，View Client 会首先使用重复数据删除功能移除将要传输的数据中的冗余数据块。接下来，View Client 会压缩剩余的数据或者确定这些数据无法压缩。

阅读 View Client with Local Mode 日志

要生成显示重复数据删除和压缩统计数字的日志条目，您必须将日志设置为 `[Debug（调试）]` 模式。

表 13-5 显示了客户端计算机上 View Client with Local Mode 日志的位置。

表 13-5 View Client with Local Mode 日志的位置

操作系统	路径
Windows 7 和 Windows Vista	`C:\Users\`*用户名*`\AppData\VMware\VDM\Logs\`
Windows XP	`C:\Documents and Settings\`*用户名*`\Local Settings\Application Data\VMware\VDM\Logs\`

检入或复制本地桌面后，View Transfer Server 会传输自上一次检出或复制后在本地桌面生成的数据。如果您了解桌面生成新数据所用的时间，您就能大致估算出数据传输的大小。下面的示例日志条目显示了自上一次检出或复制以来经过的时间（以分钟为单位）：

```
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize:Total checkin size over 34 minutes:
```

确定重复数据删除和压缩的影响

`[GetTotalCheckinSize（获取检入总大小）]` 日志条目显示了数据传输前预测的数据传输大小。这些数字涵盖本地桌面传输数据的所有磁盘。

下面的示例条目显示了在检入操作过程中不会被重复数据删除功能优化的数据量。View 预计将会传输这个数据量。

```
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize:non-dedupe:2 MB
```

在下面的示例条目中，`[parent-dedupe（父重复数据删除）]` 条目显示了在 View Transfer Server 上重复数据删除功能将优化的数据量。`[self-dedupe（自我重复数据删除）]` 条目显示了客户端计算机上重复数据删除的数据量。将这些条目中的数字相加，即可得出重复数据删除功能将会优化的数据总量。

```
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize:parent-dedupe:871 MB
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize:self-dedupe:0 MB
```

`[Replication statistics（复制统计数字）]` 日志条目显示通过网络发送的实际数据量。每个进行数据传输的本地桌面磁盘会生成单独的统计数字。

在下面的示例中，[parent-dedupe（父重复数据删除）] 和 [self-dedupe（自我重复数据删除）] 条目分别显示了 View Transfer Server 和客户端计算机上的重复数据删除统计数字。

```
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Replication statistics:
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Parent dedup:871.139 MB
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Self dedup:0.000 MB
```

下面的示例条目显示了在传输操作过程中压缩的数据量：

```
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Compression:0.000 MB compressed to 0.000 MB
```

下面的示例条目显示未压缩的数据量。

```
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm] Raw
data:2.198 MB
```

在这个示例中，本地桌面显示了诸如 "Transferring 871MB" 的消息。然而，重复数据删除减少了该数据量。尽管无法压缩剩余的数据，但是只有 2.198 MB 的数据通过网络进行传输。

针对数据传输的客户文件系统优化

在传输操作过程中，View Transfer Server 通过优化客户文件系统来减少必须通过网络发送的数据量。

当桌面虚拟机包含主 NTFS 分区时，View Transfer Server 会传输由 NTFS 分配的数据块。未分配的数据块不会被传输。该策略可最大限度减少要传输数据块的总数。

仅当传输主 NTFS 分区的数据时，才会执行客户文件系统优化。在扩展分区、Logical Disk Manager 分区、Windows 7 或 Windows Vista 虚拟机上的压缩 NTFS 卷上，View Transfer Server 不执行该优化。

客户文件系统优化与重复数据删除和数据压缩有所不同，尽管这两种技术同样能优化数据传输，但它们完全独立于桌面客户操作系统。有关这些操作的详细信息，请参见第 215 页，“优化本地桌面主机与数据中心之间的数据传输”。

配置终端的资源使用情况

默认情况下，在本地系统上检出使用的 View 桌面会利用主机的内存和 CPU 资源。桌面上的虚拟 NIC 通过 NAT 共享主机的 IP 和 MAC 地址。您可以更改此默认行为。

覆盖内存和 CPU 资源的本地使用情况

无论在 vCenter Server 中为虚拟机指定的内存和 CPU 设置是多少，本地桌面在被检出之后即可以利用本地系统的内存和 CPU 资源。您可以覆盖此默认行为。

默认情况下，对于检出在本地模式下使用的 View 桌面，为其分配的 RAM 容量会自动调整为客户端主机上可用的特定 RAM 容量。

该计算公式考虑了可供在主机和客户 View 桌面之间拆分的内存量。Windows XP 操作系统最少需要 512 MB RAM。32 位 Windows 7 或 Windows Vista 操作系统最少需要 1 GB RAM。可用于拆分的内存容量等于主机上的 RAM 总量减去主机和客户操作系统所需的最小 RAM 容量。

表 13–7 分配给本地 View 桌面的内存

内存分配	Windows XP 客户机	Windows 7 和 Vista 客户机
最小容量	512 MB	1 GB
最佳容量	512 MB +（可用容量/2）	1 GB +（可用容量/2）
最大容量	2 GB	4 GB

例如，如果一个 Windows 7 主机一共具有 2 GB RAM，则在本地运行 Windows 7 View 桌面需要 2 GB RAM，其中 1 GB RAM 分配给主机，另外 1 GB RAM 分配给本地 View 桌面。如果主机具有 3 GB RAM，则会将 1.5 GB RAM 分配给主机，另外 1.5 GB RAM 分配给本地 View 桌面。

注意 自动调整内存分配时，本地桌面的内存不会设置为小于 vCenter Server 中所配置的值。

同样，本地 View 桌面最多可以在客户端主机上使用 4 个可用 CPU。

您可以更改这些默认值并指定该设置的范围。该设置可应用于客户端上的所有本地桌面，或者根据设置应用于特定 View Connection Server 实例（特定用户有权在客户端上使用该实例）的某个特定桌面或所有桌面。

要更改这些默认值，您必须配置 Windows 注册表设置。然后可以使用组策略对象 (Group Policy Object, GPO) 等标准 Windows 工具来部署这些注册表设置。

前提条件

- 如果打算设置本地桌面可以使用的特定 CPU 数，请关闭本地桌面。
- 由于在多数情况下您可以指定该设置的范围，因此请确定您将需要指定的 ID。

表 13–6 在针对本地模式资源使用情况的注册表设置中使用的标识符

范围	变量名	描述
针对代理	*broker_guid*	用于 View Connection Server 实例或组的全局唯一标识符。使用 `vdmadmin -C` 命令可确定 GUID。请参阅第 272 页，“使用 -C 选项设置 View Connection Server 组名”。
针对用户	*remote_user_sid*	最终用户的安全 ID。在 View Connection Server 主机上使用“ADSI 编辑”实用程序，找到 **[CN=*计算机 CN*,OU=Servers,DC=vdi,DC=vmware,DC=int]** 的 **[pae-SIDString]** 字段的值。
针对桌面	*desktop_ID*	View 桌面的 ID。在 View Connection Server 上使用“ADSI 编辑”实用程序。该 ID 列在 **[DC=vdi,DC=vmware,DC=int]** 的 **[OU=Applications]** 中。桌面 ID 是使用桌面池显示名称的可区分名称：**CN=*池显示名称*,OU=Applications,DC=vdi,DC=vmware,DC=int**。

您还可以在客户端计算机的 `mvdi.lst` 文件中找到代理 GUID。在 Windows XP 上，该文件位于 `C:\Documents and Settings\`*用户名*`\Local Settings\Application Data\VMware\VDM` 文件夹中。打开该文件并搜索 `brokerGUID`。远程用户安全 ID 也列在该文件中。打开该文件并搜索 `user-sid`。

步骤

- 要覆盖默认行为以使本地桌面仅使用在 vCenter Server 中配置的内存量，需要创建并部署一个 GPO 来添加以下某个注册表项，并将其值设为 1。

设置范围	路径
整个客户端	`HKCU\Software\VMware, Inc.\VMware VDM\Client \disableOfflineDesktopMemoryScaleup`
针对代理和用户	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*代理 guid*`\`*远程用户 sid*`\disableOfflineDesktopMemoryScaleup`

  值为 1 表示 `disableOfflineDesktopMemoryScaleup` 打开，0 值则表示关闭。

- 若要设置 View 桌面在本地运行时可以使用的特定内存容量，应创建并部署一个 GPO 来添加以下注册表项之一，从而指定容量（以 MB 为单位，最高为 32 GB）。

设置范围	路径
整个客户端	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*代理 guid*`\`*远程用户 sid*`\offlineDesktopDefaultMemoryScaleupValue`
针对桌面	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*代理 guid*`\`*远程用户 sid*`\`*桌面 ID*`\offlineDesktopDefaultMemoryScaleupValue`

  如果您设置的数值过大，本地桌面将无法开机，并且会显示一条错误消息。

- 如果为桌面配置的内存超过客户端主机上可用的内存，那么要检出该桌面，就应创建并部署一个 GPO 来添加以下注册表项，从而按您的意愿指定本地桌面所需的容量（以 MB 为单位）。

  `HKCU\Software\VMware, Inc.\VMware VDM\Client\`*代理 guid*`\`*远程用户 sid*
  `\offlineDesktopReportedHostMemoryValue`

- 要覆盖默认行为以使本地桌面仅使用在 vCenter Server 中配置的 CPU 数量，需要创建并部署一个 GPO 来添加以下某个注册表项，并将其值设为 1。

设置范围	路径
整个客户端	`HKCU\Software\VMware, Inc.\VMware VDM\Client \disableOfflineDesktopCPUScaleup`
针对代理和用户	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*代理 guid*`\`*远程用户 sid*`\disableOfflineDesktopCPUScaleup`

  值为 1 表示 `disableOfflineDesktopCPUScaleup` 打开，0 值则表示关闭。

- 若要设置 View 桌面在本地运行时可以使用的特定 CPU 数量，应创建并部署一个 GPO 来添加以下注册表项之一，从而指定 CPU 数量（最多 4 个）。

设置范围	路径
整个客户端	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*代理 guid*`\`*远程用户 sid*`\offlineDesktopDefaultCPUScaleupValue`
针对桌面	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*代理 guid*`\`*远程用户 sid*`\`*桌面 ID*`\offlineDesktopDefaultCPUScaleupValue`

  如果您指定一个无效值或者指定的 CPU 数量多于主机上可用的数量，本地桌面将无法开机，并且会显示一条错误消息。如果您设置的值大于 4，将使用 4 作为其实际值。

当本地桌面开机时，这些设置就会生效，除非在设置中允许报告的所需内存容量少于 vCenter Server 中设定的容量。桌面检出后，该设置将变为只读状态。

将网络类型从 NAT 改为桥接

默认情况下，View 桌面在本地系统上检出使用后，其虚拟网络类型会变为 NAT（网络地址转换）。您可以将此行为替换成使用桥接式网络连接，以使 View 桌面在网络上具有自己的身份。

通过桥接网络连接，View 桌面中的虚拟网络适配器可连接到主机中的物理网络适配器。采用桥接网络连接，网络上的其他计算机就可以看到 View 桌面，这种网络类型要求桌面具有各自的 IP 地址。

NAT 将虚拟机配置为共享主机的 IP 和 MAC 地址。View 桌面将与客户端主机在网络中共享一个网络身份。

若要为客户端主机上的所有本地桌面或特定本地桌面更改这些默认设置，您必须配置 Windows 注册表设置。然后可以使用组策略对象 (Group Policy Object, GPO) 等标准 Windows 工具来部署这些注册表设置。

前提条件

- 由于在多数情况下您可以指定该设置的范围，因此请确定您将需要指定的 ID。

表 13–8 在针对本地模式资源使用情况的注册表设置中使用的标识符

范围	变量名	描述
针对代理	*broker_guid*	用于 View Connection Server 实例或组的全局唯一标识符。使用 `vdmadmin –C` 命令可确定 GUID。请参阅第 272 页，“使用 -C 选项设置 View Connection Server 组名”。
针对用户	*remote_user_sid*	最终用户的安全 ID。在 View Connection Server 主机上使用“ADSI 编辑”实用程序，找到 **[CN=*计算机 CN*,OU=Servers,DC=vdi,DC=vmware,DC=int]** 的 **[pae-SIDString]** 字段的值。
针对桌面	*desktop_ID*	View 桌面的 ID。在 View Connection Server 上使用“ADSI 编辑”实用程序。该 ID 列在 **[DC=vdi,DC=vmware,DC=int]** 的 **[OU=Applications]** 中。桌面 ID 是使用桌面池显示名称的可区分名称：**CN=*池显示名称*,OU=Applications,DC=vdi,DC=vmware,DC=int**。

您还可以在客户端计算机的 `mvdi.lst` 文件中找到代理 GUID。在 Windows XP 上，该文件位于 `C:\Documents and Settings\`*用户名*`\Local Settings\Application Data\VMware\VDM` 文件夹中。打开该文件并搜索 `brokerGUID`。远程用户安全 ID 也列在该文件中。打开该文件并搜索 `user-sid`。

步骤

◆ 若要覆盖默认行为，使本地桌面使用桥接网络连接，应创建并部署一个 GPO 来添加以下注册表项之一，并将其值设为 1。

设置范围	路径
整个客户端	HKCU\Software\VMware, Inc.\VMware VDM\Client \offlineDesktopUseBridgedNetworking
针对 Connection Server 和特定用户	HKCU\Software\VMware, Inc.\VMware VDM\Client*代理 guid**远程用户 sid*\offlineDesktopUseBridgedNetworking
特定桌面	HKCU\Software\VMware, Inc.\VMware VDM\Client*代理 guid**远程用户 sid**桌面 ID*\offlineDesktopUseBridgedNetworking

将值设为 1 可将桌面设置为使用桥接网络连接。将值设为 0 即可使用默认的 NAT 模式。

当最终用户启动本地桌面时，所做的设置就会生效。

配置 HTTP 缓存以通过 WAN 部署本地桌面

您可以使用 HTTP 缓存实现链接克隆本地桌面的部署。配置 HTTP 缓存对于通过 WAN 连接到数据中心的远程和分支办公机构都有益处。HTTP 缓存可以减少通过 WAN 传输 View Composer 基础映像的性能成本。

如果您将链接克隆桌面配置为在远程办公室使用本地模式，您的 WAN 可能不具有足够的带宽来将 View Composer 基础映像直接下载到每个本地计算机。例如，重复传输 6 GB 基础映像的操作可能会被禁止。

如果您设置一个 HTTP 缓存，当第一个用户检出桌面时，基础映像将被存储在代理服务器的缓存中。当后续用户检出桌面时，基础映像将通过本地办公室的 LAN 来传输。

要完成检出操作，View Transfer Server 仍然必须通过 WAN 从数据中心传输每个用户的链接克隆操作系统磁盘和永久磁盘，但这些磁盘的大小远小于基础映像。

1 配置 View Connection Server 以支持 HTTP 缓存 View Composer 基础映像第 223 页，

   要允许缓存代理服务器在本地桌面和数据中心之间传递 View Composer 基础映像和其他数据，您必须在 View Connection Server 中配置特定设置。

2 限制基础映像程序包文件的大小以允许缓存第 224 页，

   View Composer 基础映像程序包可以包含大于一千兆字节的文件，这样的大小已远远超出了很多代理服务器的缓存限制。您可以配置 View Transfer Server 来将基础映像程序包分成不大于代理服务器缓存容量的文件。

3 将客户端计算机配置为通过代理服务器传输数据第 225 页，

   要支持 HTTP 缓存，您必须将托管本地桌面的客户端计算机配置为通过缓存代理服务器传输桌面数据。您还必须将客户端计算机配置为使用代理服务器的 HTTP 地址进行 Internet 连接。

4 配置代理服务器以缓存 View Composer 基础映像第 225 页，

   当您设置代理服务器以支持本地桌面的 HTTP 缓存时，必须配置该缓存的容量和 HTTP 连接方法。

配置 View Connection Server 以支持 HTTP 缓存 View Composer 基础映像

要允许缓存代理服务器在本地桌面和数据中心之间传递 View Composer 基础映像和其他数据，您必须在 View Connection Server 中配置特定设置。

您可以使用两种不同的 View 设置来为以下两种数据配置 SSL 加密：

- View Composer 基础映像
- 其他链接克隆桌面数据，包括操作系统磁盘和永久磁盘

对于从 Transfer Server 存储库到本地计算机的基础映像程序包文件传输，您必须禁用其 SSL 加密。禁用 SSL 可允许代理服务器访问并缓存程序包文件内容。禁用 SSL 不会公开基础映像数据。当您将基础映像发布到 Transfer Server 存储库时，数据会被加密；当数据通过 WAN 下载到代理服务器时，数据仍然保持加密状态。

您可以选择是否对其他所有本地桌面数据的传输使用 SSL 加密。要允许通过缓存代理服务器传输其他本地桌面数据，您必须将代理服务器配置为允许使用 HTTP CONNECT 方法，或者为 View Connection Server 上的本地模式操作启用 SSL 加密。

如果您使用 SSL 加密，则不必更改代理服务器设置，但 SSL 加密可以影响链接克隆操作系统磁盘和永久磁盘的数据传输性能。

在每个将 View 服务交付给配置了 HTTP 缓存的客户端的 View Connection Server 实例上，您都必须配置这些 SSL 设置。

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 在 [View Server] 面板中，选择一个 View Connection Server 实例，然后单击 **[Edit（编辑）]**。

3 取消选中 **[Use SSL when provisioning desktops in Local Mode（部署本地模式桌面时使用 SSL）]**。

   该设置会为将基础映像程序包文件从 Transfer Server 存储库下载到本地计算机的操作禁用 SSL。

4 如果您不将缓存代理服务器设置为使用 HTTP CONNECT 方法，则需要选择 **[Use SSL for Local Mode operations（为本地模式操作使用 SSL）]**。

   该设置会影响其他所有本地桌面数据的传输。

限制基础映像程序包文件的大小以允许缓存

View Composer 基础映像程序包可以包含大于一千兆字节的文件，这样的大小已远远超出了很多代理服务器的缓存限制。您可以配置 View Transfer Server 来将基础映像程序包分成不大于代理服务器缓存容量的文件。

在 Transfer Server 存储库中发布程序包时，View Transfer Server 会创建指定大小的程序包文件。在将程序包发布到存储库之前，您必须配置其大小限制。View Transfer Server 不会根据大小限制来拆分现有程序包文件。

您可以在副本组中的任何 View Connection Server 实例上设置该值。更改 View LDAP 时，所做更改会传播给所有副本 View Connection Server 实例。

前提条件

熟悉如何在 `vdmadmin` 命令中使用 -T 选项。请参阅第 288 页，“使用 -T 选项设置发布 View Transfer Server 文件包的拆分限制”。

步骤

1 在您的 View Connection Server 计算机上启动 Windows 命令提示符。

2 键入 `vdmadmin` 命令以及 -T 选项。

```
vdmadmin -T [-packagelimit 以字节为单位的大小]
```

   默认情况下，`vdmadmin` 命令可执行文件的路径为 `C:\Program Files\VMware\VMware View\Server\tools\bin`。

示例 13–1 设置程序包文件大小限制

将程序包文件拆分限制设为 10 KB。

```
vdmadmin -T -packagelimit 10240
```

显示当前程序包文件的拆分限制。

```
vdmadmin -T
```

将客户端计算机配置为通过代理服务器传输数据

要支持 HTTP 缓存，您必须将托管本地桌面的客户端计算机配置为通过缓存代理服务器传输桌面数据。您还必须将客户端计算机配置为使用代理服务器的 HTTP 地址进行 Internet 连接。

要允许数据通过代理服务器进行传输，您需要在客户端计算机上添加相应的注册表项。您可以在 Active Directory 中创建一个组策略，以便在域中的多个计算机上设置该注册表项。

步骤

1 在本地模式客户端系统上启动 Windows 注册表编辑器。

2 在左侧窗格中，展开注册表路径。

处理器	描述
64 位	**[HKEY_LOCAL_MACHINE] > [SOFTWARE] > [Wow6432Node] > [VMware Inc.] > [VMware VDM]**
32 位	**[HKEY_LOCAL_MACHINE] > [SOFTWARE] > [VMware Inc.] > [VMware VDM]**

3 单击 **[Edit（编辑）] > [New（新建）] > [String Value（字符串值）]**，在新的值条目中键入 `useProxyForTransfer`。

4 右键单击 **[useProxyForTransfer]** 条目，然后单击 **[Modify（修改）]**，键入 **true** 并单击 **[OK（确定）]**。

该条目即被添加到注册表中。

5 退出 Windows 注册表编辑器。

6 在客户端计算机上，将 Internet Explorer 连接设置配置为使用您的缓存代理服务器。

   a 启动 Internet Explorer，单击 **[Tools（工具）] > [Internet Options（Internet 选项）]**。

   b 选择 **[Connections（连接）]** 选项卡，单击 **[LAN Settings（局域网设置）]**。

   c 单击 **[Use a proxy server for your LAN（为 LAN 使用代理服务器）]**，然后单击 **[Advanced（高级）]**。

   d 为 HTTP 连接、安全连接、FTP 连接和 Socks 连接键入代理地址和端口号，然后单击 **[OK（确定）]**。

配置代理服务器以缓存 View Composer 基础映像

当您设置代理服务器以支持本地桌面的 HTTP 缓存时，必须配置该缓存的容量和 HTTP 连接方法。

前提条件

- 验证您通过 `vdmadmin -T` 命令设置的基础映像程序包文件的大小限制。请参阅第 224 页，“限制基础映像程序包文件的大小以允许缓存”。
- 确认您是否为本地模式操作使用 SSL。请参阅第 223 页，“配置 View Connection Server 以支持 HTTP 缓存 View Composer 基础映像”。

步骤

1 在代理服务器上配置缓存的最大大小。

要计算最大大小，请考虑本地桌面使用的 View Composer 基础映像的数量和大小。基础映像作为程序包文件下载到代理服务器。还要考虑您计划在代理服务器上缓存的其他文件。

2 配置可以缓存的最大单个文件的大小。

代理服务器上单个文件的最大大小不能低于您通过 `vdmadmin -T` 命令设置的程序包文件的最大大小。

3 如果您没有为 View Connection Server 启用 **[Use SSL for Local Mode operations（为本地模式操作使用 SSL）]** 设置，请将代理服务器上的访问控制列表 (ACL) 设置为开放端口 80 并允许使用 CONNECT 方法连接端口 80。

View Transfer Server 使用 CONNECT 方法通过代理服务器提供安全加密链路连接。View Transfer Server 使用该连接在本地桌面和数据中心之间传输文件和数据（而非 View Composer 基础映像）。使用端口 80 提高传输性能。

配置本地桌面客户端计算机的检测信号时间间隔

托管本地桌面的客户端计算机会按固定的时间间隔向 View Connection Server 发送检测消息以读取其检出桌面的状态。所有客户端计算机的默认检测信号时间间隔都是 5 分钟。您可以更改所有客户端计算机的检测信号时间间隔，也可以为特定客户端计算机设置不同的检测信号时间间隔。

- 更改所有本地桌面客户端计算机的检测信号时间间隔第 226 页，

  要更改托管本地桌面的所有客户端计算机的检测信号时间间隔，您可以在 View Connection Server 主机上使用“ADSI 编辑”实用程序来编辑 View LDAP。“ADSI 编辑”实用程序随 View Connection Server 一起安装。

- 设置特定本地桌面客户端计算机的检测信号时间间隔第 227 页，

  要为托管本地桌面的特定客户端计算机设置检测信号时间间隔，需要在该计算机上使用 Windows 注册表编辑器编辑系统注册表。

更改所有本地桌面客户端计算机的检测信号时间间隔

要更改托管本地桌面的所有客户端计算机的检测信号时间间隔，您可以在 View Connection Server 主机上使用“ADSI 编辑”实用程序来编辑 View LDAP。“ADSI 编辑”实用程序随 View Connection Server 一起安装。

在 View Connection Server 实例上更改 View LDAP 时，所作更改会传播给所有副本 View Connection Server 实例。

前提条件

请参阅 Microsoft TechNet 网站，了解如何在您的 Windows Server 操作系统版本上使用“ADSI 编辑”实用程序。

步骤

1 在您的 View Connection Server 主机上启动“ADSI 编辑”实用程序。

2 选择或连接到 **[DC=vdi, DC=vmware, DC=int]**。

3 在对象 **[CN=Common, OU=Global, OU=Properties]** 上，将 **[pae-mVDIOfflineUpdateFrequency]** 属性设置为新的检测信号时间间隔（以分钟计）。

您必须键入一个正整数。默认情况下未设置该属性。未设置该属性时，默认的间隔值是 5 分钟。

新的检测信号时间间隔会在托管本地桌面的客户端计算机下次向 View Connection Server 发送检测消息时生效。您无需重新启动 View Connection Server 服务或客户端计算机。

如果客户端计算机上设置的检测信号时间间隔值较小，View 会使用客户端计算机的值而非 View Connection Server 的值。默认情况下，客户端计算机上不会设置检测信号时间间隔。

设置特定本地桌面客户端计算机的检测信号时间间隔

要为托管本地桌面的特定客户端计算机设置检测信号时间间隔，需要在该计算机上使用 Windows 注册表编辑器编辑系统注册表。

如果客户端计算机上设置的检测信号时间间隔大于 View Connection Server 主机上设置的间隔，View 就不会使用客户端计算机上设置的检测信号时间间隔。View 始终使用这两个值中较小的值。View Connection Server 的默认检测信号时间间隔是 5 分钟。

前提条件

请参阅 Microsoft TechNet 网站，了解如何在本地模式客户端系统的 Windows 操作系统版本上使用 Windows 注册表编辑器。

步骤

1 在本地桌面客户端计算机上启动 Windows 注册表编辑器。

2 新建一个名为 **policyUpdateFrequency** 的注册表项。

系统注册表的位置取决于客户端计算机的处理器类型。

选项	操作
64 位	将 **[policyUpdateFrequency]** 添加到 **[HKEY_LOCAL_MACHINE] > [SOFTWARE] > [Wow6432Node] > [VMware Inc.] > [VMware VDM]**。
32 位	将 **[policyUpdateFrequency]** 添加到 **[HKEY_LOCAL_MACHINE] > [SOFTWARE] > [VMware Inc.] > [VMware VDM]**。

3 将 **policyUpdateFrequency** 项的值设为新的检测信号时间间隔（以毫秒为单位）。

您必须键入一个正整数。

将本地桌面手动下载到网络连接较差的位置

对带宽极为有限的网络用户来说，检出桌面的操作可能已被禁止，因为您必须下载几千兆字节的数据。要为这些用户提供服务，您可以手动下载桌面文件并将其复制到客户端计算机。

例如，住在乡村的用户可以使用拨号网络连接在家办公。用户可能不会前往主要办公地点工作，而他们在那里可以通过 LAN 将桌面检出到用户的笔记本电脑。

在这种情况下，您可以将桌面文件手动下载到便携式设备（如 USB 设备或 DVD）。在将设备提交给用户之后，用户可将文件复制到客户端计算机上指定的目录中并从 View 数据中心检出桌面。

此方法仅可用于 View Composer 链接克隆桌面。

- 您可以手动下载 View Composer 基础映像文件。
- 当用户检出桌面时，仍然必须通过网络下载链接克隆操作系统磁盘和永久磁盘文件。

然而，基础映像中包含了最大的文件。例如，Windows 7 基础映像的大小可能为 6 GB 到 10 GB。操作系统磁盘和永久磁盘的容量要远小于这个值。

1 从 Transfer Server 存储库复制基础映像第 228 页，

要将桌面手动下载到客户端计算机以在本地模式中使用，您必须将 View Composer 基础映像复制到便携式设备。基础映像作为程序包发布在 Transfer Server 存储库中。

2 将基础映像文件复制到客户端计算机第 228 页，

要将桌面手动下载到客户端计算机以在本地模式中使用，您必须将基础映像程序包文件从便携设备复制到客户端计算机。

3 设置权限以允许 View 使用复制的程序包文件第 229 页，

要允许检出操作在本地模式中进行，必须为复制到客户端计算机上检出目录中的基础映像文件设置权限。

4 手动复制基础映像后检出桌面第 229 页，

将基础映像手动复制到客户端计算机并设置了程序包文件权限之后，必须指导用户检出桌面。

从 Transfer Server 存储库复制基础映像

要将桌面手动下载到客户端计算机以在本地模式中使用，您必须将 View Composer 基础映像复制到便携式设备。基础映像作为程序包发布在 Transfer Server 存储库中。

前提条件

- 确认您已对 View Manager 进行配置，以部署本地桌面。请参阅第 199 页，"本地桌面部署设置概述"。
- 确认您创建了一个链接克隆桌面池并将程序包发布到了 Transfer Server 存储库。请参阅第 208 页，"在 Transfer Server 存储库中发布程序包文件"。

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Transfer Server Repository（Transfer Server 存储库）]**。

2 在 [Contents（内容）] 窗格中，选择与您检出的桌面所在桌面池相关的程序包并单击 **[Details（详细信息）]**。

3 确认该桌面池与该程序包相关。

4 找到 [Repository（存储库）] 路径（包括程序包 ID）。

例如：`\\mycomputer.com\ImageRepository\Published\f222434a-e52a-4ce3-92d1-c14122fca996`

5 将 Transfer Server 存储库的程序包内容复制到便携设备。

您必须将整个程序包目录复制到便携设备。

将基础映像文件复制到客户端计算机

要将桌面手动下载到客户端计算机以在本地模式中使用，您必须将基础映像程序包文件从便携设备复制到客户端计算机。

前提条件

- 确认用户已在客户端计算机上安装 View Client with Local Mode。
- 确认您已将程序包文件复制到便携设备。请参阅第 228 页，"从 Transfer Server 存储库复制基础映像"。

步骤

1 将包含桌面池内程序包文件的便携设备交付给用户。

2 将程序包文件复制到客户端计算机上指定的检出目录。

将文件复制到使用桌面池显示名称的检出目录中的子目录中。例如，要从名为 `LocalPool` 的桌面池下载文件，请将文件复制到*检出目录*`\LocalPool`。

检出目录	描述
Windows 7 和 Windows Vista 上的默认目录	`C:\Users\`*用户名*`\AppData\Local\VMware\VDM\Local Desktops\`*池显示名称*
Windows XP 上的默认目录	`C:\Documents and Settings\`*用户名*`\Local Settings\Application Data\VMware\VDM\Local Desktops\`*池显示名称*
自定义目录	您可以指定您自己的目录。例如，要从名为 `LocalPool` 的桌面池下载文件，您可以创建以下路径：`C:\CheckOutDirectory\LocalPool`。

设置权限以允许 View 使用复制的程序包文件

要允许检出操作在本地模式中进行，必须为复制到客户端计算机上检出目录中的基础映像文件设置权限。

您必须移除程序包文件的只读属性，并提供对其所在目录及所有文件的 **Full control（完全控制）** 特权。

以下示例描述了如何在 Windows 7 计算机上设置权限。其他操作系统上的设置步骤可能稍有不同。

前提条件

确认您已将程序包文件复制到客户端计算机上的目录中。请参阅第 228 页，“将基础映像文件复制到客户端计算机”。

步骤

1 登录 Windows 7 客户操作系统，单击 **[Libraries（库）]** 图标并导航到检出目录。

2 右键单击检出目录，然后单击 **[Properties（属性）]**。

3 单击 **[Security（安全）]** 选项卡，然后单击 **[Edit（编辑）]**。

4 在组或用户名列表中，选择将检出桌面的用户的名称。

   如果用户名不在列表中，请单击 **[Add（添加）]** 添加该用户名。

5 查看 **[Allow（允许）]** 列中的 **[Full control（完全控制）]**，然后单击 **[OK（确定）]**。

6 单击 **[General（常规）]** 选项卡，取消选中 **[Read-only (Only applies to files in folder)（只读（仅应用于文件夹中的文件））]**。

   确保完全取消选中该复选框。

7 在 [Confirm Attribute Changes（确认属性更改）] 对话框中，选中 **[Apply changes to this folder, subfolders and files（将更改应用于此文件夹、子文件夹和文件）]**，然后单击 **[OK（确定）]**。

手动复制基础映像后检出桌面

将基础映像手动复制到客户端计算机并设置了程序包文件权限之后，必须指导用户检出桌面。

前提条件

- 确认 View Client with Local Mode 已安装在客户端计算机上。
- 确认您设置了相应权限，能够使用复制到客户端计算机的程序包文件。请参阅第 229 页，“设置权限以允许 View 使用复制的程序包文件”。

步骤

1 在客户端计算机上，启动 Vmware View Client，连接到 View Connection Server，登录 View Connection Server 并选择一个桌面池。

2 单击桌面池旁边的下拉箭头按钮并单击 **[Check out（检出）]**。

3 （可选）如果您将程序包文件复制到自定义目录，请将 View Client 配置为将桌面检出到该自定义目录。

a 在 [Check Out（检出）] 对话框中，单击 **[Options（选项）]**。

b 在 [Check-out（检出）] 目录旁边，单击 **[Browse（浏览）]** 并选择包含池名称文件夹的目录。

不要选择池名称文件夹本身。

例如，如果您将名为 `LocalPool` 的池中的程序包文件复制到 `C:\CheckOutDirectory\LocalPool` 目录，则请选择 `C:\CheckOutDirectory` 目录。

c 单击 **[OK（确定）]**。

4 在 [Check Out（检出）] 对话框中，单击 **[OK（确定）]**。

View Manager 会检出桌面。View Transfer Server 会检测到基础映像文件驻留在客户端计算机中并仅下载剩余的桌面文件。这些文件包括操作系统磁盘和永久磁盘文件（如配置）。

排除 View Transfer Server 和本地桌面操作问题

对于常见的 View Transfer Server 和本地桌面操作问题，您可以从故障排除提示中获得帮助。

- 检出失败，显示“无可用的 Transfer Server”错误第 231 页，

  用户尝试检出桌面时，操作会失败并显示一条错误信息 `[No available Transfer Server`（无可用的 `Transfer Server`）`]`。

- 初始检出后的桌面检出问题第 232 页，

  假定 View Transfer Server 可正常运行，您可能会发现出现检出问题的原因在于 View Connection Server 不再具有本地计算机的加密密钥。

- 登录窗口需要较长时间才能显示第 232 页，

  在某些情况下，您打开 View Client 并指定某个 View Connection Server 实例后，登录窗口需要 30 秒或更长时间才能显示。

- View Transfer Server 保持在正在等待处理状态第 233 页，

  View Transfer Server 长时间保持在 [Pending（正在等待处理）] 状态且不可用。例如，[Pending（正在等待处理）] 状态可能持续十分钟以上。

- View Transfer Server 无法进入维护模式第 233 页，

  当您试图将 View Transfer Server 置于维护模式时，它会长时间保持在 [Maintenance mode pending（维护模式正在等待处理）] 状态。

- Transfer Server 存储库无效第 233 页，

  在 View Administrator 中，View Transfer Server 显示为 [Bad Transfer Server repository（无效的 Transfer Server 存储库）] 状态。

- View Transfer Server 无法连接到 Transfer Server 存储库第 234 页，

  在 View Administrator 中，View Transfer Server 显示为 [Repository Connection Error（存储库连接错误）] 状态。

- View Transfer Server 无法进行运行状况检查第 234 页，

  在 View Administrator 中，View Transfer Server 显示为 [Bad Health Check（无效的运行状况检查）] 状态。View Administrator 仪表板在 View Transfer Server 旁显示了一个向下的红色箭头。

- 缺少 Transfer Server 存储库第 235 页，

  在 View Administrator 中，View Transfer Server 显示 [Missing Transfer Server Repository（缺少 Transfer Server 存储库）] 状态。

- View Transfer Server 实例具有冲突的 Transfer Server 存储库第 235 页，

  在 View Administrator 中，View Transfer Server 实例显示 [Transfer Server Repository Conflict（Transfer Server 存储库冲突）] 状态。

- View Transfer Server Web 服务处于关闭状态第 236 页，

  在 View Administrator 中，View Transfer Server 显示 [Web Server Down（Web 服务器关闭）] 状态。

- 本地桌面的虚拟磁盘需要修复第 236 页，

  您可能需要修复本地桌面的虚拟磁盘。

- 从本地桌面恢复数据第 237 页，

  VMware View 通过对其所有的虚拟磁盘进行加密来保护本地桌面的虚拟机。如果虚拟机的检出标识符已从配置中删除，或者会话或策略文件已损坏，您可能无法启动或检入本地桌面。您可以对本地桌面的虚拟机进行解密，以便从中恢复数据。

检出失败，显示“无可用的 Transfer Server”错误

用户尝试检出桌面时，操作会失败并显示一条错误信息 `[No available Transfer Server（无可用的 Transfer Server）]`。

问题

View Transfer Server 开始向客户端计算机传输数据之前，操作完成约 10% 的时候，检出可能失败。在后面的过程中检出也可能失败。例如，基础映像可能已传输到客户端计算机上，但是不能传输其他虚拟机磁盘。

由特定 View Transfer Server 实例管理的所有检出操作都会发生该问题。

原因

发生该问题的原因是 View Transfer Server 在一个无法访问桌面驻留的数据存储的 ESX 主机上运行。在检出操作过程中，View Transfer Server 从数据存储向客户端计算机传输桌面数据。这些数据存储必须可从运行 View Transfer Server 虚拟机的 ESX 主机进行访问。

解决方案

- 将 View Transfer Server 虚拟机迁移到可以访问数据存储的 ESX 主机上。

  a 在 View Administrator 中，将 View Transfer Server 实例置于维护模式。

  b 在 vSphere Client 中，使用 [Migration（迁移）] 向导将 View Transfer Server 虚拟机迁移到目标 ESX 主机上。

  c 在 View Administrator 中，选择 View Transfer Server 实例并退出维护模式。

- 如果您无法迁移 View Transfer Server 虚拟机，请在可以访问数据存储的 ESX 主机的另一台虚拟机上重新创建 View Transfer Server。

  a 在 View Administrator 中，从 View Manager 中移除 View Transfer Server 实例。

  b 在 vSphere Client 中，卸载 View Transfer Server 或移除 View Transfer Server 虚拟机。

  c 在目标 ESX 主机上创建新的虚拟机。

  d 在虚拟机上安装 View Transfer Server。

  e 在 View Administrator 中，将 View Transfer Server 添加到 View Manager。

  有关安装 View Transfer Server 的更多信息，请参阅《*VMware View 安装指南*》。

初始检出后的桌面检出问题

假定 View Transfer Server 可正常运行，您可能会发现出现检出问题的原因在于 View Connection Server 不再具有本地计算机的加密密钥。

问题

成功检出并检入本地桌面后，您再次检出该桌面时无法连接到本地桌面。您可能会看到如下错误消息：`Cannot access local desktop--desktop corrupted`（无法访问本地桌面，桌面已损坏）。

原因

如果您更改本地桌面的加密密钥密码，或是从其所在的池中删除了该桌面并创建了一个新桌面，View Connection Server 将使用新的身份验证密钥来生成一个新的配置文件。

最终用户尝试再次检出桌面时，只会下载更改过的文件。下载的新文件使用新的加密密钥，但本地计算机上的旧文件仍使用旧的加密密钥，但 View Connection Server 不再拥有旧密钥。

解决方案

- 最终用户必须删除所有本地桌面文件才能再次检出桌面。

  文件夹位于本地桌面检出目录下。下载首个本地桌面时，如果您未单击 **[Options（选项）]** 并更改本地桌面的存储目录，那么它们就存储在默认的检出目录下。

桌面操作系统	默认检出目录
Windows 7 和 Windows Vista 上的默认目录	`C:\Users\`*用户名*`\AppData\Local\VMware\VDM\Local Desktops\`*池显示名称*
Windows XP 上的默认目录	`C:\Documents and Settings\`*用户名*`\Local Settings\Application Data\VMware\VDM\Local Desktops\`*池显示名称*

登录窗口需要较长时间才能显示

在某些情况下，您打开 View Client 并指定某个 View Connection Server 实例后，登录窗口需要 30 秒或更长时间才能显示。

问题

登录窗口有时长达 30 秒无法访问，直到连接尝试超时。

原因

如果 View Client 为 View Connection Server 使用 IP 地址，那么当您拥有网络连接但无法访问 View Connection Server 时，就会发生此类问题。例如，当拥有 Internet 连接却不具备允许访问 View Connection Server 的 VPN 连接时，如果您试图在家中登录本地桌面，则将遇到此类问题。

如果 View Client 在局域网 (LAN) 中使用主机名而非 IP 地址，则发生此类问题意味着 View Connection Server 或代理（如果您使用代理）处于关闭状态或者防火墙阻止了连接。在广域网 (WAN) 中，发生此类问题可能意味着同样的情况，也可能表明主机名在公共 DNS 中可解析但无法通过 WAN 访问服务器。

解决方案

您必须等到连接尝试超时。登录窗口最终将会显示。

View Transfer Server 保持在正在等待处理状态

View Transfer Server 长时间保持在 [Pending（正在等待处理）] 状态且不可用。例如，[Pending（正在等待处理）] 状态可能持续十分钟以上。

问题

将 View Transfer Server 添加到 View Manager 之后，View Transfer Server 的状态未更改为 [Ready（就绪）]。

原因

常见的原因是 View Connection Server 无法连接到 View Transfer Server。

解决方案

- 确认已在虚拟机上安装 View Transfer Server。
- 确认 View Transfer Server 服务正在运行。
  a 在 View Transfer Server 虚拟机上，打开 **[Control Panel（控制面板）] > [Administrative Tools（管理工具）] > [Services（服务）]** 对话框。
  b 确保 VMware View Transfer Server 服务、VMware View Transfer Server Control 服务和 VMware View Framework Component 服务已启动。
- 确保 View Transfer Server 虚拟机能够解析 View Connection Server 主机名。
- 确保 View Connection Server 虚拟机可对 View Transfer Server 的 IP 地址执行 ping 操作。
- 确认 View Transfer Server 虚拟机可以满足推荐的系统配置。请参阅*《VMware View 安装指南》*中的 View Transfer Server 系统要求。

View Transfer Server 无法进入维护模式

当您试图将 View Transfer Server 置于维护模式时，它会长时间保持在 [Maintenance mode pending（维护模式正在等待处理）] 状态。

问题

当 View Transfer Server 处于 [Maintenance mode pending（维护模式正在等待处理）] 状态时，您无法执行将 Transfer Server 存储库迁移到新位置等操作，直到 View Transfer Server 进入维护模式后才能执行。

原因

活动传输操作或将程序包发布到 Transfer Server 存储库的操作仍在进行中。

解决方案

等待活动数据传输和发布操作完成。当所有操作完成时，View Transfer Server 会进入维护模式。

Transfer Server 存储库无效

在 View Administrator 中，View Transfer Server 显示为 [Bad Transfer Server repository（无效的 Transfer Server 存储库）] 状态。

问题

当 View Transfer Server 处于该状态时，您无法对链接克隆桌面执行传输操作或发布程序包。

原因

View Transfer Server 需要连接的 Transfer Server 存储库与当前在 View Connection Server 中配置的 Transfer Server 存储库不同。

无效的 Transfer Server 存储库迁移也可能会使 View Transfer Server 进入该状态。

解决方案

再次将 Transfer Server 存储库迁移到新位置。有关详细说明，请参阅第 210 页，“将 Transfer Server 存储库迁移到新位置”。

View Transfer Server 无法连接到 Transfer Server 存储库

在 View Administrator 中，View Transfer Server 显示为 [Repository Connection Error（存储库连接错误）] 状态。

问题

View Transfer Server 无法连接在 View Connection Server 中配置的 Transfer Server 存储库。

原因

Transfer Server 存储库配置无效。如果存储库配置在网络共享位置，则网络路径或凭据无效。如果存储库配置在本地位置，则文件系统路径无效。

解决方案

1 将所有 View Transfer Server 实例置于维护模式。

   a 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

   b 选择一个 View Transfer Server 实例。

   c 如果传输正处于活动状态，在将该 View Transfer Server 实例置于维护模式之前，需要选择是取消活动传输还是等待活动传输完成。

   d 单击 **[OK（确定）]**。

   e 对所有的 View Transfer Server 实例重复这些步骤。

2 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Transfer Server Repository（Transfer Server 存储库）]**。

3 单击 **[Edit（编辑）]** 并重新配置 Transfer Server 存储库。

   View Transfer Server 会验证 Transfer Server 存储库是否有效。

View Transfer Server 无法进行运行状况检查

在 View Administrator 中，View Transfer Server 显示为 [Bad Health Check（无效的运行状况检查）] 状态。View Administrator 仪表板在 View Transfer Server 旁显示了一个向下的红色箭头。

问题

在 [Bad Health Check（无效的运行状况检查）] 状态下，View Transfer Server 无法正常工作。您无法执行传输操作或在 Transfer Server 存储库中发布程序包。

原因

View Transfer Server 不可用、未运行或无法正常工作。

解决方案

- 确认已在虚拟机上安装 View Transfer Server。
- 确认 View Transfer Server 服务正在运行。
  a 在 View Transfer Server 虚拟机上，打开 **[Control Panel（控制面板）] > [Administrative Tools（管理工具）] > [Services（服务）]** 对话框。
  b 确保 VMware View Transfer Server 服务、VMware View Transfer Server Control 服务和 VMware View Framework Component 服务已启动。
- 确保 View Transfer Server 虚拟机能够解析 View Connection Server 主机名。
- 确保 View Connection Server 虚拟机可对 View Transfer Server 的 IP 地址执行 ping 操作。
- 确认 View Transfer Server 虚拟机可以满足推荐的系统配置。请参阅 *《VMware View 安装指南》*中的 View Transfer Server 系统要求。

缺少 Transfer Server 存储库

在 View Administrator 中，View Transfer Server 显示 [Missing Transfer Server Repository（缺少 Transfer Server 存储库）] 状态。

问题

您无法对链接克隆桌面执行传输操作或在 Transfer Server 存储库中发布程序包。

原因

未在 View Manager 中配置 Transfer Server 存储库。

解决方案

1 将所有 View Transfer Server 实例置于维护模式。
  a 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。
  b 选择一个 View Transfer Server 实例。
  c 如果传输正处于活动状态，在将该 View Transfer Server 实例置于维护模式之前，需要选择是取消活动传输还是等待活动传输完成。
  d 单击 **[OK（确定）]**。
  e 对所有的 View Transfer Server 实例重复这些步骤。
2 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Transfer Server Repository（Transfer Server 存储库）]**。
3 单击 **[Edit（编辑）]** 并配置 Transfer Server 存储库。

  View Transfer Server 会验证 Transfer Server 存储库是否有效。

View Transfer Server 实例具有冲突的 Transfer Server 存储库

在 View Administrator 中，View Transfer Server 实例显示 [Transfer Server Repository Conflict（Transfer Server 存储库冲突）] 状态。

问题

您无法对链接克隆桌面执行传输操作或在 Transfer Server 存储库中发布程序包。

原因

多个 View Transfer Server 实例被配置为连接到不同的 Transfer Server 存储库。

如果同时将多个 View Transfer Server 实例添加到了 View Manager 中，并为每个实例配置不同的 Transfer Server 存储库，就可能出现此状态。

解决方案

从 View Manager 移除 View Transfer Server 实例并一次添加一个实例。如果某个 View Transfer Server 实例显示 [Bad Transfer Server Repository（无效的 Transfer Server 存储库）] 状态，请参阅第 233 页，“Transfer Server 存储库无效”中的故障排除信息。

View Transfer Server Web 服务处于关闭状态

在 View Administrator 中，View Transfer Server 显示 [Web Server Down（Web 服务器关闭）] 状态。

问题

View Transfer Server 无法从 Transfer Server 存储库下载程序包，并且无法将其他桌面数据传输到本地桌面。

原因

支持 Transfer Server 存储库的 Apache2.2 Web 服务未运行。

解决方案

1 在 View Transfer Server 虚拟机上，打开 **[Control Panel（控制面板）]** > **[Administrative Tools（管理工具）]** > **[Services（服务）]** 对话框。
2 启动 Apache2.2 服务。

本地桌面的虚拟磁盘需要修复

您可能需要修复本地桌面的虚拟磁盘。

问题

您试图连接至本地桌面时，将看到一条错误消息。例如：

`Cannot open the disk 'C:\Documents and Settings\jo\Local Settings\Application Data\View\Local Desktops\Win7_32b_Local_Mode\52411f5e05b854ca-b5c54521f6010b22-scsi00-000002.vmdk' or one of the snapshot disks it depends on.`（无法打开磁盘“`C:\Documents and Settings\jo\Local Settings\Application Data\View\Local Desktops\Win7_32b_Local_Mode\52411f5e05b854ca-b5c54521f6010b22-scsi00-000002.vmdk`”或者该磁盘依赖的其中一个快照磁盘。）

`Reason:The specified disk needs repair.`（原因：指定磁盘需要修复。）

原因

如果您在虚拟机映像正在更新时断开连接或者关闭客户端计算机，就会发生此类问题。

解决方案

1 您可以通过在命令行指定 `[-repairLocalDesktops]` 选项来启动 View Client。

   例如：

   ```
   wswc -desktopName lmdt01 -userName jo -domainName MYDOM -repairLocalDesktops
   ```

   修复过程需要几分钟时间。
2 如果修复过程失败，请回滚本地会话并检出一个新的本地桌面。

从本地桌面恢复数据

VMware View 通过对其所有的虚拟磁盘进行加密来保护本地桌面的虚拟机。如果虚拟机的检出标识符已从配置中删除，或者会话或策略文件已损坏，您可能无法启动或检入本地桌面。您可以对本地桌面的虚拟机进行解密，以便从中恢复数据。

重要事项 只有在您使用任何其他方法都无法恢复本地桌面的数据时再执行以下步骤。

View Connection Server 实例必须能够访问 View LDAP 配置，该配置保存了本地桌面的身份验证密钥。

根据您希望恢复的数据量，您可以选择解密整个虚拟机或其中一个组成磁盘。如果解密单个磁盘，则解密过程将会较快。

前提条件

- 确认您无法在不丢失数据的情况下回滚本地桌面。
- 确认本地桌面的数据没有复制或保存在另一个位置。
- 以 **Administrators** 用户角色登录到安装有 View Connection Server 实例的 Windows 计算机。
- 确保您要执行解密操作的文件夹有足够的空间存储加密和解密的虚拟机文件，并且您拥有该文件夹的写入权限。

步骤

1 从客户机中将虚拟机文件复制到 View Connection Server 实例的本地文件夹中。

   重要事项 不要通过网络共享位置或映射的驱动器访问这些文件。

2 要解密文件，请运行 `vdmadmin` 命令。

```
vdmadmin -V -rescue -d <桌面> -u <域>\<用户> -infile <VM 文件路径>
```

选项	描述
-d <*桌面*>	指定桌面池名称。
-infile <*VM 文件路径*>	为本地桌面的虚拟机指定虚拟机文件的路径。 要恢复整个虚拟机，您可以作为 `-infile` 选项的自变量来指定 VMware 虚拟机配置文件（VMX 文件）的名称。 要恢复虚拟机的某个磁盘，您可以作为 `-infile` 选项的自变量来为该磁盘指定 VMware 虚拟磁盘文件（VMDK 文件）的名称。不要指定与磁盘分区相对应的 VMDK 文件。
-u <*域*>\<*用户*>	指定本地桌面最终用户的域和名称。

`vdmadmin` 命令将解密的虚拟机文件写入名为 `rescued` 的子文件夹。

示例 13–2 解密虚拟机文件

通过指定虚拟机的 VMX 文件来解密整个虚拟机。

```
vdmadmin -V -rescue -d lmdtpool -u MYCORP\jo -infile "J:\Temp\LMDT_Recovery
\CN=lmdtpool,OU=Applications,DC=mycorp,DC=com.vmx"
```

列出本地桌面虚拟机的 `scsi00` 磁盘可用的文件。

```
J:\Temp\LMDT_Recovery>dir /b *scsi00*
52e52b7c26a2f683-42b945f934e0fbb2-scsi00-000001.vmdk
52e52b7c26a2f683-42b945f934e0fbb2-scsi00-000001-s001.vmdk
52e52b7c26a2f683-42b945f934e0fbb2-scsi00-000001-s002.vmdk
52e52b7c26a2f683-42b945f934e0fbb2-scsi00-000001-s003.vmdk
52e52b7c26a2f683-42b945f934e0fbb2-scsi00-000001-s004.vmdk
5215df4df635a14d-caf14c8dbbb14a3d-scsi00.vmdk
5215df4df635a14d-caf14c8dbbb14a3d-scsi00-s001.vmdk
5215df4df635a14d-caf14c8dbbb14a3d-scsi00-s002.vmdk
5215df4df635a14d-caf14c8dbbb14a3d-scsi00-s003.vmdk
5215df4df635a14d-caf14c8dbbb14a3d-scsi00-s004.vmdk
```

通过指定 VMDK 文件来解密当前版本的 `scsi00` 磁盘。

```
vdmadmin -V -rescue -d lmdtpool -u MYCORP\jo -infile "J:\Temp\LMDT_Recovery
\52e52b7c26a2f683-42b945f934e0fbb2-scsi00-000001.vmdk"
```

下一步

使用 VMware Workstation 来开启并检查解密的整个虚拟机，或者使用 VMware DiskMount 来装载解密的磁盘。另外，也可以通过将解密磁盘的 VMDK 文件附加到 VMware Workstation 的虚拟机上来检查解密磁盘的内容。从虚拟机文件恢复数据之后，请回滚本地桌面。

维护 View 组件 14

为保持 View 组件可用并正常运行，您可以执行多种维护任务。

本章讨论了以下主题：

备份和还原 View 配置数据

通过在 View Administrator 中计划或运行自动备份，您可以备份 View Manager 和 View Composer 配置数据。通过手动导入备份的 View LDAP 文件和 View Composer 数据库文件，可以还原 View 配置。

您可以利用备份与还原功能保存和迁移 View 配置数据。

备份 View Connection Server 和 View Composer 数据

完成对 View Connection Server 的初始配置后，您应当计划对 View Manager 和 View Composer 配置数据进行定期备份。您可以使用 View Administrator 来保留 View Manager 和 View Composer 数据。

View Manager 将 View Connection Server 配置数据存储在 View LDAP 存储库中。View Composer 将链接克隆桌面的配置数据存储在 View Composer 数据库中。

当您使用 View Administrator 执行备份时，View Manager 会备份 View LDAP 配置数据和 View Composer 数据库。两个备份文件集都存储在同一位置。View LDAP 数据将以 LDAP 数据交换格式 (LDIF) 导出。有关 View LDAP 的说明，请参阅第 20 页，“View LDAP 目录”。

View Manager 可以从任何 View Connection Server 实例中导出配置数据。

如果您的副本实例组中有多个 View Connection Server 实例，则只需从一个实例中导出数据。所有副本实例均包含相同的配置数据。

不要将 View Connection Server 副本实例作为备份机制。如果 View Manager 将各个 View Connection Server 副本实例中的数据同步，那么一个实例中的任何数据丢失可能会导致所有组成员中均丢失相应数据。

如果 View Connection Server 结合使用多个 vCenter Server 实例和多种 View Composer 服务，那么 View Manager 会备份与 vCenter Server 实例关联的所有 View Composer 数据库。

您可以通过多种方式来执行备份。

- 使用 View Manager 配置备份功能可计划自动备份。
- 使用 View Administrator 中的 **[Backup Now（立即备份）]** 功能可即刻开始备份。
- 使用 `vdmexport` 工具手动导出 View LDAP 数据。每个 View Connection Server 实例均附带了此工具。

注意 `vdmexport` 工具仅备份 View LDAP 数据。此工具不会备份 View Composer 数据库信息。

计划 View Manager 配置备份

您可计划定期备份 View Manager 配置数据。View Manager 将备份 View LDAP 存储库（View Connection Server 实例用其存储配置数据）的内容。

选择 View Connection Server 实例并单击 **[Backup Now（立即备份）]**，即可立即备份配置。

前提条件

熟悉备份设置。请参阅第 240 页，“View Manager 配置备份设置”。

步骤

1 在 View Administrator 中，单击 **[Configuration（配置）] > [Servers（服务器）]**。

2 选择要备份的 View Connection Server 实例，单击 **[Edit（编辑）]**。

3 指定 [View Manager Configuration Backup（View Manager 配置备份）] 设置，以配置备份频率、最大备份数以及备份文件所在的文件夹位置。

4 单击 **[OK（确定）]**。

View Manager 配置备份设置

View Manager 可以定期备份 View Connection Server 和 View Composer 配置数据。您可以在 View Administrator 中设置备份操作的频率和其他设置。

表 14–1 View Manager 配置备份设置

设置	描述
Automatic backup frequency（自动备份频率）	[Every Hour（每小时）]：每小时整点进行备份。 [Every 6 Hour（每 6 小时）]：在零点、上午 6 点、中午 12 点和下午 6 点进行备份。 [Every 12 Hour（每 12 小时）]：在零点和中午 12 点进行备份。 [Every Day（每天）]：每天零点进行备份。 [Every 2 Days（每 2 天）]：在星期六、星期一、星期三和星期五的零点进行备份。 [Every Week（每周）]：在每周星期六的零点进行备份。 [Every 2 Weeks（每 2 周）]：在每隔一周的星期六零点进行备份。 [Never（从不）]：不自动进行备份。
Max number of backups（最大备份数量）	View Connection Server 实例上可以存储的最大备份文件数。该数必须是大于 0 的整数。 达到最大数量时，View Manager 会删除最早的备份文件。 此设置还适用于您使用 **[Backup Now（立即备份）]** 功能创建的备份文件。
Folder location（文件夹位置）	备份文件的位置。 默认位置是运行 View Connection Server 的计算机上的以下路径。 ■ 在 Windows Server 2008 计算机上：`C:\Programdata\VMWare\VDM\backups` ■ 在 Windows Server 2003 计算机上：`C:\Documents and Settings\All Users\Application Data\VMWare\VDM\backups` 当您使用 **[Backup Now（立即备份）]** 功能时，View Manager 也会将备份文件存储在该位置。

从 View Connection Server 中导出配置数据

您可以通过导出 View Connection Server 实例的 View LDAP 存储库内容来备份其配置数据。

使用 `vdmexport` 命令将数据导出到 LDIF 文件中。您可以在任意 View Connection Server 实例上运行 `vdmexport` 命令。

如果您的副本实例组中有多个 View Connection Server 实例，则只需从一个实例中导出数据。所有副本实例均包含相同的配置数据。

注意 `vdmexport` 命令仅备份 View LDAP 数据。此命令不会备份 View Composer 数据库信息。

前提条件

- 从以下默认路径中找出随 View Connection Server 安装的 `vdmexport.exe` 命令可执行文件。

  ```
  C:\Program Files\VMware\VMware View\Server\tools\bin
  ```

- 以 Administrators 或 Administrators (Read only) 用户角色登录 View Connection Server 实例。

步骤

1 选择 **[Start（开始）] > [Command Prompt（命令提示符）]**。

2 在命令提示符下，键入 `vdmexport` 命令，并将输出重定向至文件。

  例如：

  ```
  vdmexport > Myexport.LDF
  ```

  您可以作为 `-f` 参数的自变量指定输出文件的名称。

  例如：

  ```
  vdmexport -f Myexport.LDF
  ```

`vdmexport` 命令会将 View Connection Server 配置数据写入指定的 LDIF 文件中。

有关 `vdmexport` 命令的更多信息，请参阅《*VMware View Integration Guide*》（VMware View 集成指南）。

下一步

您可以通过以下方式使用 LDIF 文件来维护配置数据。

- 还原或传输 View Connection Server 的配置信息。
- 通过编辑文件中的条目和将文件导入目标 View Connection Server 实例，可以修改 View Connection Server 的配置信息。

有关导入 LDIF 文件的详细信息，请参阅第 241 页，“还原 View Connection Server 和 View Composer 配置数据”。

还原 View Connection Server 和 View Composer 配置数据

您可以手动还原由 View Manager 备份的 View Connection Server LDAP 配置文件和 View Composer 数据库文件。

您需要手动运行单个实用程序来还原 View Connection Server 和 View Composer 配置数据。

还原配置数据前，请确认您在 View Administrator 中备份了配置数据。请参阅第 239 页，“备份 View Connection Server 和 View Composer 数据”。

使用 vdmimport 实用程序将 View Connection Server 数据从 LDIF 备份文件导入到 View Connection Server 实例中的 View LDAP 存储库。

您可以使用 SviConfig 实用程序将 View Composer 数据从 .svi 备份文件导入到 View Composer SQL 数据库中。

将配置数据导入 View Connection Server 中

您可以通过导入 LDIF 文件中存储的数据备份副本，来还原 View Connection Server 实例的配置数据。

使用 vdmimport 命令将 LDIF 文件的数据导入到 View Connection Server 实例中的 View LDAP 存储库。

有关备份 View LDAP 存储库的信息，请参阅第 239 页，“备份 View Connection Server 和 View Composer 数据”。

前提条件

- 从以下默认路径中找出随 View Connection Server 安装的 vdmimport 命令可执行文件。

  C:\Program Files\VMware\VMware View\Server\tools\bin

- 以 Administrators 用户角色登录 View Connection Server 实例。

步骤

1 选择 **[Start（开始）] > [Command Prompt（命令提示符）]**。

2 在命令提示符下，键入 vdmimport 命令，指定一个现有的 LDIF 文件作为 -f 参数的赋值。

  例如：

  vdmimport -f Myexport.LDF

vdmimport 命令将使用该 LDIF 文件中的配置数据更新 View Connection Server 中的 View LDAP 存储库。

有关 vdmimport 命令的更多信息，请参阅 *《VMware View Integration Guide》*（VMware View 集成指南）。

还原 View Composer 数据库

您可以将备份的 View Composer 配置文件导入存储链接克隆信息的 View Composer 数据库中。

使用 SviConfig restoredata 命令，您可以在系统出现故障后还原 View Composer 数据库，或是将 View Composer 配置恢复到某个早期状态。

重要事项 只有经验丰富的 View Composer 管理员才能使用 SviConfig 实用程序。此实用程序用于解决与 View Composer 服务相关的问题。

前提条件

确认 View Composer 数据库备份文件的位置。默认情况下，View Manager 将备份文件存储在 View Connection Server 计算机的 C:驱动器中：

- 在 Windows Server 2008 计算机上：C:\Programdata\VMWare\VDM\backups
- 在 Windows Server 2003 计算机上：C:\Documents and Settings\All Users\Application Data\VMWare \VDM\backups

View Composer 备份文件采用带日期时间戳和 .svi 后缀的命名约定。

Backup-*<年><月><日><计数>*-*<vCenter Server 名称>*_*<域名>*.svi

例如：Backup-20090304000010-foobar_test_org.svi

步骤

1 将 View Composer 备份文件从 View Connection Server 计算机复制到可被安装了 View Composer 服务的 vCenter Server 计算机访问的某个位置。

2 在 vCenter Server 计算机上，停止 VMware View Composer 服务。

3 在 vCenter Server 计算机上，打开 Windows 命令提示符，并导航至 `SviConfig` 可执行文件。

   该文件与 View Composer 应用程序位于同一位置。

```
C:\Program Files\VMware\VMware View Composer\sviconfig.exe
```

4 运行 `SviConfig restoredata` 命令。

```
sviconfig -operation=restoredata
-DsnName=<目标数据库源名 (DSN)>
-Username=<数据库管理员用户名>
-Password=<数据库管理员密码>
-BackupFilePath=<View Composer 备份文件的路径>
```

   例如：

```
sviconfig -operation=restoredata -dsnname=LinkedClone
-username=Admin -password=Pass
-backupfilepath="C:\Program Files\VMware\VMware View
Composer\Backup-20090304000010-foobar_test_org.SVI"
```

5 启动 VMware View Composer 服务。

下一步

有关 `SviConfig restoredata` 命令的输出结果代码，请参阅第 243 页，“还原 View Composer 数据库的结果代码”。

还原 View Composer 数据库的结果代码

还原 View Composer 数据库时，`SviConfig restoredata` 命令会返回一个结果代码。

表 14–2 Restoredata 结果代码

代码	描述
0	操作成功结束。
1	找不到所提供的 DSN。
2	提供的数据库管理员凭据无效。
3	数据库的驱动程序不受支持。
4	出现异常问题，命令无法完成。
14	另一个应用程序正在使用 View Composer 服务。执行命令前，请关闭该服务。
15	还原过程中出现问题。屏幕上的日志输出会提供详细信息。

监视 View 组件

使用 View Administrator 仪表板可以快速浏览 View 部署中 View Manager 和 vSphere 组件的状态。

View Administrator 显示有关 View Connection Server 实例、事件数据库、安全服务器、View Composer 服务、数据存储、vCenter Server 实例和域的监视信息。

注意 View Manager 不能确定 Kerberos 域的状态信息。即使配置了 Kerberos 域且其可以正常运行，View Administrator 也会将 Kerberos 域的状态显示为未知。

步骤

1 在 View Administrator 中，单击 **[Dashboard（仪表板）]**。

2 在 [System Health（系统运行状况）] 窗格中，展开 **[View components（View 组件）]**、**[vSphere components（vSphere 组件）]** 或者 **[Other components（其他组件）]**。

- 绿色向上箭头表明组件没有问题。
- 红色向下箭头表明组件不可用或未运行。
- 黄色双箭头表明组件处于警告状态。
- 问号表明组件状态未知。

3 单击组件的名称。

将出现一个对话框显示名称、版本、状态和其他组件信息。

监视桌面状态

使用 View Administrator 仪表板可以快速浏览 View 部署中桌面的状态。例如，您可以显示所有断开连接的桌面或处于维护模式下的桌面。

前提条件

熟悉桌面状态。请参阅第 170 页，“虚拟机的桌面状态”。

步骤

1 在 View Administrator 中，单击 **[Dashboard（仪表板）]**。

2 在 [Desktop Status（桌面状态）] 窗格中，展开一个状态文件夹。

选项	描述
Preparing（正在准备）	列出当虚拟机处于部署、删除或维护模式时的桌面状态。
Problem Desktops（问题桌面）	列出桌面错误状态。
Prepared for use（已准备好，可供使用）	列出当桌面可供使用时的桌面状态。

3 定位桌面状态，并单击旁边带超链接的数字。

[Desktops（桌面）] 页面将显示所有处于选定状态的桌面。

下一步

您可以单击某个桌面名称查看桌面的详细信息，也可以单击 View Administrator 后退箭头返回到仪表板页面。

了解 View Manager 服务

View Connection Server 实例和安全服务器的运行依赖于系统上运行的若干服务。这些系统是自动启动和停止的，但您有时需要手动调整这些服务的运行。

您可以使用 Microsoft Windows 服务工具来停止或启动 View Manager 服务。如果您停止 View Connection Server 主机或安全服务器上的 View Manager 服务，最终用户将无法再登录他们的桌面，直到您重新启动服务。如果服务停止运行，或者它所控制的 View Manager 功能不响应，可能也要重新启动服务。

停止和启动 View 服务

View Connection Server 实例和安全服务器的运行依赖于系统上运行的若干服务。在排除 VMware View 的运行故障时，有时需要手动停止和启动这些服务。

如果您停止了 View 服务，最终用户将无法登录他们的桌面。您应该在计划的系统维护时间执行这种操作，或者警告最终用户其桌面会暂时不可用。

注意 仅停止 View Connection Server 主机上的 VMware View Connection Server 服务或安全服务器上的 VMware View Security Server 服务。不要停止任何其他组件服务。

前提条件

熟悉 View Connection Server 主机和安全服务器上运行的服务，如第 245 页，“View Connection Server 主机上的服务”和第 246 页，“安全服务器上的服务”中所述。

步骤

1 在命令提示符中输入 `services.msc`，启动 Windows Services 工具。

2 选择 View Connection Server 主机上的 VMware View Connection Server 服务或安全服务器上的 VMware View Security Server 服务，然后根据需要单击 **[Stop（停止）]**、**[Restart（重新启动）]** 或 **[Start（启动）]**。

3 确认所列服务的状态按预期发生了更改。

View Connection Server 主机上的服务

View Manager 的运行依赖于 View Connection Server 主机上运行的若干服务。如果您想调整这些服务的运行，就需要先熟悉这些服务。

表 14–3 View Connection Server 主机服务

服务名称	启动类型	描述
VMware View Connection Server	自动	提供连接代理服务。必须运行此服务 View Manager 才能正常运行。如果启动或停止此服务，会同时启动或停止 Framework、Message Bus、Security Gateway 和 Web 服务。此服务不会启动或停止 VMwareVDMDS 服务或 VMware View 脚本主机服务。
VMware View Framework 组件	手动	为 View Manager 提供事件日志、安全和 COM+ 框架服务。必须运行此服务 View Manager 才能正常运行。
VMware View Message Bus 组件	手动	在 View Manager 组件之间提供消息传递服务。必须运行此服务 View Manager 才能正常运行。
VMware View 脚本主机	自动（如果已启用）	对您删除虚拟机时运行的第三方脚本提供支持。默认情况下，此服务已被禁用。如果您需要运行脚本，应启用此服务。
VMware View Security Gateway 组件	手动	为 View Manager 提供安全加密链路服务。必须运行此服务 View Manager 才能正常运行。
VMware View Web 组件	手动	为 View Manager 提供 Web 服务。必须运行此服务 View Manager 才能正常运行。
VMwareVDMDS	自动	为 View Manager 提供 LDAP 目录服务。必须运行此服务 View Manager 才能正常运行。升级 VMware View 期间也必须运行此服务，以确保正确迁移现有数据。

安全服务器上的服务

View Manager 的运行依赖于安全服务器上运行的若干服务。如果您想调整这些服务的运行，就需要先熟悉这些服务。

表 14–4　安全服务器服务

服务名称	启动类型	描述
VMware View Security Server	自动	提供安全服务器服务。必须运行此服务，安全服务器才能正确运行。如果您启动或停止此服务，会同时启动或停止 Framework 和 Security Gateway 服务。
VMware View Framework 组件	手动	提供事件日志、安全和 COM+ 框架服务。必须运行此服务，安全服务器才能正确运行。
VMware View Security Gateway 组件	手动	提供安全加密链路服务。必须运行此服务，安全服务器才能正确运行。

View Transfer Server 主机上的服务

本地桌面的传输操作依赖于 View Transfer Server 主机上运行的服务。如果您想调整这些服务的运行，就需要先熟悉这些服务。

View Transfer Server 上安装的所有服务都必须运行，才能保证 View Manager 中本地桌面的正确运行。

表 14–5 View Transfer Server 主机服务

服务名称	启动类型	描述
VMware View Transfer Server	自动	提供协调 View Transfer Server 相关服务的服务。如果您启动或停止此服务，会同时启动或停止 View Transfer Server Control 服务和 Framework 服务。
VMware View Transfer Server Control 服务	手动	为 View Transfer Server 提供管理能力并处理与 View Connection Server 的通信。
VMware View Framework 组件	手动	为 View Manager 提供事件日志、安全和 COM+ 框架服务。
Apache2.2 服务	自动	为以本地模式运行 View 桌面的客户端计算机提供数据传输能力。 当您将 View Transfer Server 添加到 View Manager 时，Apache2.2 服务即会启动。

为 VMware View 添加许可证

如果系统中当前的许可证到期，或者您要访问当前未经许可的 VMware View 功能，则可以使用 View Administrator 来添加许可证。

您可以在 View Manager 运行过程中为 VMware View 添加许可证。无需重新启动系统，对桌面的访问也不会中断。

前提条件

要成功操作 View Manager 及其加载功能（如 View Composer 和本地桌面），请获取有效的许可密钥。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Product licensing and usage（产品许可和使用情况）]**，然后单击 **[Edit license（编辑许可证）]**。

2 输入许可证序列号，然后单击 **[OK（确定）]**。

[Product Licensing（产品许可）] 窗口将显示更新的许可信息。

从 Active Directory 更新常规用户信息

您可以用 Active Directory 中存储的当前用户信息来更新 View Manager。此功能可更新 View 用户的姓名、电话、电子邮件、用户名和默认的 Windows 域。还会更新受信任的外部域。

当您要修改 Active Directory 中的受信任外部域列表，尤其是域之间的信任关系改变会影响 View Manager 中的用户权限时，请使用此功能。

此功能会扫描 Active Directory 中的最新用户信息，并刷新 View Manager 配置。

您也可以使用 `vdmadmin` 命令更新用户和域信息。请参阅第 273 页，“使用 -F 选项更新外部安全主体”。

步骤

1 在 View Administrator 中，单击 **[Users and Groups（用户和用户组）]**。

2 选择要更新所有用户的信息还是单个用户的信息。

选项	操作
针对所有用户	单击 **[Update General User Information（更新常规用户信息）]**。 更新所有用户和用户组可能需要较长时间。
针对单个用户	a 单击要更新的用户名。 b 单击 **[Update General User Information（更新常规用户信息）]**。

使用现有数据库迁移 View Composer

在某些情况下，您可能需要将 View Composer 服务迁移到新的计算机上。但可以继续使用现有 View Composer 数据库。

例如，您可以将 vCenter Server 实例迁移到新的 ESX 主机或群集上以扩展部署或者从硬件故障中恢复。要保留链接克隆桌面，您还必须迁移随 vCenter Server 安装的 View Composer 服务。

要迁移 View Composer 服务，您需要在旧的计算机上卸载该服务，然后在新的计算机上安装该服务。有关安装说明，请参阅 *《VMware View 安装指南》*。

必须在安装新的 View Composer 服务的计算机所在的域或受信任域中的某个可用计算机上配置现有 View Composer 数据库。

View Composer 会创建 RSA 密钥对来加密和解密 View Composer 数据库中存储的身份验证信息。要使该数据源与新的 View Composer 服务兼容，必须迁移由原来的 View Composer 服务创建的 RSA 密钥容器。您必须将 RSA 密钥容器导入到安装新服务的计算机上。

注意 每个 View Composer 服务实例必须具有各自的 View Composer 数据库。多个 View Composer 实例不能共享一个 View Composer 数据库。

准备 Microsoft .NET Framework 以迁移 RSA 密钥

要使用现有的 View Composer 数据库，就必须在计算机之间迁移 RSA 密钥容器。您可以使用 Microsoft .NET Framework 提供的 ASP.NET IIS 注册工具迁移 RSA 密钥容器。

前提条件

从以下地址下载 .NET Framework，了解 ASP.NET IIS 注册工具：

- http://www.microsoft.com/net
- http://msdn.microsoft.com/library/k6h9cz8h(VS.80).aspx

步骤

1 在安装了与现有数据库关联的 View Composer 服务的计算机上安装 .NET Framework。

2 在您要安装新 View Composer 服务的目标计算机上安装 .NET Framework。

下一步

将 RSA 密钥容器迁移到目标计算机上。请参阅第 248 页，“将 RSA 密钥容器迁移至新的 View Composer 服务”。

将 RSA 密钥容器迁移至新的 View Composer 服务

要使用现有的 View Composer 数据库，您必须将 RSA 密钥容器从现有 View Composer 服务所在的源计算机迁移到要安装新 View Composer 服务的 vCenter Server 计算机上。

您必须在安装新的 View Composer 服务之前执行此操作。

前提条件

确认源计算机和目标计算机上已安装 Microsoft .NET Framework 和 ASP.NET IIS 注册工具。请参阅第 247 页，“准备 Microsoft .NET Framework 以迁移 RSA 密钥”。

步骤

1 在现有 View Composer 服务所在的源计算机中打开一个命令提示符，并导航至 `%windir%\Microsoft.NET\Framework\v2.0`*xxxxx* 目录。

2 键入 `aspnet_regiis` 命令从而将 RSA 密钥对保存在本地文件中。

   `aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri`

   ASP.NET IIS 注册工具会将 RSA 公-私密钥对从 `SviKeyContainer` 容器导出到 `keys.xml` 文件，并在本地保存该文件。

3 将 `keys.xml` 文件复制到要安装新 View Composer 服务的目标计算机中。

4 在目标计算机上打开一个命令提示符并导航至 `%windir%\Microsoft.NET\Framework\v2.0`*xxxxx* 目录。

5 键入 `aspnet_regiis` 命令迁移 RSA 密钥对数据。

   `aspnet_regiis -pi "SviKeyContainer" "`*path*`\keys.xml"`

   其中，*path* 是导出文件的路径。

   注册工具会将密钥对数据导入本地密钥容器。

下一步

在目标 vCenter Server 计算机上安装新 View Composer 服务。有关安装说明，请参阅《*VMware View 安装指南*》。

对 View 组件进行故障排除 15

您可以采取多种操作来诊断和修复在使用 View Manager、View Composer 和 View Client 过程中可能遇到的问题。

管理员在使用 View Manager 和 View Composer 时可能会遇到异常情况，用户在使用 View Client 访问其桌面时可能会遇到困难。您可以采取故障排除操作来调查问题原因并尝试自行解决问题，也可以从 VMware 技术支持部门获取帮助。

本章讨论了以下主题：

监视系统运行状况

您可以使用 View Administrator 中的系统运行状况仪表板来快速查看是否存在影响 View 运行或最终用户桌面访问的问题。

位于 View Administrator 屏幕左上角的系统运行状况仪表板提供了一些链接，您可以通过这些链接查看 View Manager 的运行报告：

Remote Sessions（远程会话）
提供指向 [Global Remote Sessions（全局远程会话）] 屏幕的链接，该屏幕会显示有关远程会话状态的信息。

Local Sessions（本地会话）
提供指向 [Global Local Sessions View（全局本地会话视图）] 屏幕的链接，该屏幕会显示有关本地桌面会话状态的信息。

Problem Desktops（问题桌面）
提供指向 [Global Desktop View（全局桌面视图）] 屏幕的链接，该屏幕会显示被 View Manager 标记为有问题的桌面的相关信息。

Events（事件）
提供指向已过滤出错误事件和警告事件的 [Events（事件）] 屏幕的链接。

System Health（系统运行状况）
提供指向 [Dashboard（仪表板）] 屏幕的链接，该屏幕会显示 View 组件、vSphere 组件、域和桌面的状态摘要，以及数据存储的使用情况。

系统运行状况仪表板将针对每个项目显示一个标有数字的链接。该值表示所链接的报告提供了多少个项目的详细信息。

监视 View Manager 中的事件

事件数据库存储了 View Connection Server 主机或组、View Agent 以及 View Administrator 中所发生事件的相关信息，并在仪表板中显示事件数量。您可以在 [Events（事件）] 屏幕上查看事件的详细信息。

注意 事件会在 View Administrator 界面上持续显示一段有限的时间。这段时间过后，这些事件仅在历史记录数据库表中可用。您可以使用 Microsoft SQL Server 或 Oracle 数据库报告工具来查看数据库表中的事件。有关更多信息，请参阅《*VMware View Integration Guide*》（VMware View 集成指南）。

前提条件

根据《*VMware View 安装指南*》中的描述创建和配置事件数据库。

步骤

1 在 View Administrator 中，选择 **[Monitoring（监视）] > [Events（事件）]**。

2 （可选）在 [Events（事件）] 窗口中，您可以选择事件的时间范围，对事件应用过滤器，并在一个或多个栏中对列出的事件进行排序。

View Manager 事件消息

每当系统状态变化或者遇到问题时，View Manager 均会报告发生的事件。您可以根据事件消息中的信息来采取适当措施。

表 15-1 显示了 View Manager 所报告事件的类型。

表 15–1 View Manager 报告的事件类型

事件类型	描述
Audit Failure（审核失败）或 Audit Success（审核成功）	报告管理员或用户对 VMware View 的操作或配置所做的更改是否成功。
Error（错误）	报告 View Manager 所执行的错误操作。
Information（信息）	报告 VMware View 内的正常操作。
Warning（警告）	报告在操作或配置设置中，今后有可能导致更严重问题的轻微问题。

如果您看到与 [Audit Failure（审核失败）]、[Error（错误）] 或 [Warning（警告）] 事件相关的消息，则可能需要采取相应的措施。对于 [Audit Success（审核成功）] 或 [Information（信息）] 事件，则不需要采取措施。

向桌面用户发送消息

有些情况下，您可能需要向当前已登录桌面的用户发送消息。例如，如果您需要对某个桌面执行维护，则可以要求用户临时注销，或者警告他们服务将会中断。

步骤

1 在 View Administrator 中，选择 **[Users and Groups（用户和用户组）]**。

2 单击要对其发送消息的用户。

3 在 **[Sessions（会话）]** 选项卡下，选择用户会话，然后单击 **[Send Message（发送消息）]**。

4 键入消息，选择消息类型，然后单击 **[OK（确定）]**。

显示存在可疑问题的桌面

您可以通过列表显示 View Manager 检测到的可疑桌面。

View Administrator 会显示出现以下问题的桌面：

- 已开机但没有响应。
- 长时间保持部署状态。
- 已就绪但报告中指出不接受连接。
- 在 vCenter Server 中丢失。
- 当前有用户登录控制台、有未经授权的用户登录，或者未通过 View Connection Server 实例登录。

步骤

1 在 View Administrator 中，选择 **[Desktops（桌面）]**。

2 在 **[VirtualCenter VMs（VirtualCenter 虚拟机）]** 选项卡中，单击 **[Problem Desktops（问题桌面）]**。

下一步

您应当采取的措施取决于 View Administrator 所报告的桌面问题。

- 如果桌面已开机但没有响应，应重新启动该桌面的虚拟机。如果桌面仍没有响应，则需要检验桌面操作系统是否支持该 View Agent 版本。请参阅第 270 页，“使用 -A 选项配置 View Agent 日志”。
- 如果桌面长时间保持部署状态，应删除其虚拟机并重新克隆。请确认有足够的磁盘空间用来部署桌面。请参阅第 260 页，“虚拟机长时间处于“部署”状态”。
- 如果桌面报告其已经就绪，但不接受连接，请检查防火墙配置，确保显示协议（RDP 或 PCoIP）未被阻止。请参阅第 257 页，“桌面与 View Connection Server 实例之间的连接问题”。

- 如果 vCenter Server 中缺少某个桌面，请确认是否已在预期的 vCenter Server 上配置其虚拟机，或者该桌面是否已被移到另一个 vCenter Server 上。
- 如果桌面上当前有用户登录，但不是在控制台上登录，则必定是远程会话。如果无法联系已登录的用户，则可能需要重新启动虚拟机以强行注销这些用户。

管理未授权用户的桌面和相应策略

您可以显示分配给授权已被移除的用户的桌面，还可以显示应用到未授权用户的策略。

未授权用户可能已永久离开组织，或者您在较长时间内暂停了他们的帐户。尽管已经为他们分配了桌面，但他们不再具有使用桌面池的权限。

您也可以使用 vdmadmin 命令显示未授权的桌面和策略。请参阅第 282 页，“使用 -O 和 -P 选项显示未授权用户的桌面和策略”。

步骤

1. 在 View Administrator 中，选择 **[Desktops（桌面）]**。
2. 选择 **[More Commands（更多命令）] > [View Unentitled Machines（查看未授权的计算机）]**。
3. 移除未授权用户的桌面分配并回滚其检出的本地桌面。
4. 根据需要选择 **[More Commands（更多命令）] > [View Unentitled Machines（查看未授权的计算机）]** 或者 **[More Commands（更多命令）] > [View Unentitled Policies（查看未授权的策略）]**。
5. 更改或移除应用于未授权用户的策略。

收集 VMware View 的诊断信息

您可以收集诊断信息以协助 VMware 技术支持部门诊断并解决 VMware View 存在的问题。

您可以收集 VMware View 中各个组件的诊断信息。具体的信息收集方式取决于特定 VMware View 组件。

- 为 View Agent 创建数据收集工具捆绑包第 252 页，

  为协助 VMware 技术支持部门对 View Agent 进行故障排除，您可能需要使用 vdmadmin 命令来创建数据收集工具 (Data Collection Tool, DCT) 捆绑包。
- 保存 View Client 的诊断信息第 253 页，

  如果您在使用 View Client 时遇到问题，且无法采用常规的网络故障排除技术来解决问题，可以保存一个日志文件和配置相关信息的副本。
- 收集 VMware Composer 的诊断信息第 253 页，

  您可以使用 View Composer 支持脚本来收集 View Composer 的配置数据，并生成日志文件。这些信息有助于 VMware 客户支持部门诊断 View Composer 出现的问题。
- 收集 VMware Connection Server 的诊断信息第 254 页，

  您可以使用支持工具设置 View Connection Server 的日志级别并生成日志文件。
- 收集 View Agent、View Client 或 View Connection Server 的诊断信息第 255 页，

  如果您能够直接访问控制台，可以使用支持脚本为 View Connection Server、View Client 或运行 View Agent 的桌面生成日志文件。这些信息有助于 VMware 技术支持部门诊断这些组件出现的问题。

为 View Agent 创建数据收集工具捆绑包

为协助 VMware 技术支持部门对 View Agent 进行故障排除，您可能需要使用 vdmadmin 命令来创建数据收集工具 (Data Collection Tool, DCT) 捆绑包。

您必须以 **Administrators** 角色登录 View Connection Server 的标准实例或副本实例。

步骤

◆ 要指定输出捆绑包文件、桌面池和计算机的名称，请使用 `vdmadmin` 命令并附带 `-outfile`、`-d` 和 `-m` 选项。

```
vdmadmin -A [-b <身份验证自变量>] -getDCT -outfile <本地文件> -d <桌面> -m <计算机>
```

此命令可将捆绑包写入指定的输出文件中。

示例 15–1 为 View Agent 创建捆绑包文件

为桌面池 dtpool2 中的虚拟机 machine1 创建 DCT 捆绑包，并将其写入 zip 文件 `C:\myfile.zip` 中。

```
vdmadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

下一步

如果您当前存在支持请求，可以通过附加 DCT 捆绑包文件来更新请求。

保存 View Client 的诊断信息

如果您在使用 View Client 时遇到问题，且无法采用常规的网络故障排除技术来解决问题，可以保存一个日志文件和配置相关信息的副本。

在保存诊断信息并联系 VMware 技术支持部门之前，您可以先尝试解决 View Client 连接问题。有关更多信息，请参阅第 256 页，“View Client 与 View Connection Server 之间的连接问题”。

步骤

1 在 View Client 中，单击 **[Support Information（支持信息）]**，或在虚拟桌面菜单中选择 **[Options（选项）] > [Support Information（支持信息）]**。

2 在 [Support Information（支持信息）] 窗口中单击 **[Collect Support Data（收集支持数据）]**，在系统提示时单击 **[Yes（是）]**。

   将出现一个命令窗口，其中了显示收集信息的进度。此过程可能需要几分钟时间。

3 在命令窗口中，通过执行以下操作响应系统提示：输入 View Connection Server 实例（您希望针对这些实例测试 View Client 的配置）的 URL，并且在需要的情况下选择生成 VMware View 进程的诊断转储。

   这些信息将写入客户机桌面文件夹下的 zip 文件中。

4 在 VMware 网站的支持页面中提交支持请求，并附加输出 zip 文件。

收集 VMware Composer 的诊断信息

您可以使用 View Composer 支持脚本来收集 View Composer 的配置数据，并生成日志文件。这些信息有助于 VMware 客户支持部门诊断 View Composer 出现的问题。

前提条件

登录到安装有 View Composer 的 vCenter Server。

由于您必须使用 Windows 脚本宿主实用程序 (`cscript`) 运行支持脚本，因此需要熟悉 `cscript` 的使用方法。请参阅 http://technet.microsoft.com/library/bb490887.aspx。

步骤

1 打开命令提示符窗口，然后转到 `C:\Program Files\VMware\VMware View Composer` 目录。

如果您未将软件安装在默认目录中，请替换相应的驱动器盘符和路径。

2 键入命令以运行 `svi-support` 脚本。

```
cscript ".\svi-support.wsf /zip"
```

您可以使用 `/?` 选项显示脚本可用的其他命令选项的相关信息。

运行脚本后，系统将向您显示输出文件的名称和位置。

3 在 VMware 网站的支持页面中提交支持请求，并附加输出文件。

收集 VMware Connection Server 的诊断信息

您可以使用支持工具设置 View Connection Server 的日志级别并生成日志文件。

支持工具可用来收集 View Connection Server 的日志数据。这些信息有助于 VMware 技术支持部门诊断 View Connection Server 出现的问题。支持工具不可用于收集 View Client 或 View Agent 的诊断信息，您必须改为使用支持脚本。请参阅第 255 页，“收集 View Agent、View Client 或 View Connection Server 的诊断信息”。

前提条件

以 **Administrators** 角色登录 View Connection Server 的标准实例或副本实例。

步骤

1 选择 **[Start（开始）]** > **[All Programs（所有程序）]** > **[VMware]** > **[Set View Connection Server Log Levels（设置 View Connection Server 日志级别）]**。

2 在 **[Choice（选项）]** 文本框中键入一个数值以设置日志级别，然后按 Enter 键。

选项	描述
0	将日志级别重置为默认值。
1	选择常规日志级别（默认）。
2	选择调试日志级别。
3	选择完整日志级别。

您通常需要输入 **2** 来选择调试日志级别。

系统将按您选择的详细信息级别开始记录日志信息。

3 当您针对 View Connection Server 行为收集了足够信息后，可选择 **[Start（开始）]** > **[All Programs（所有程序）]** > **[VMware]** > **[Generate View Connection Server Log Bundle（生成 View Connection Server 日志捆绑包）]**。

支持工具可将日志文件写入 View Connection Server 实例桌面上名为 `vdm-sdct` 的文件夹中。

4 在 VMware 网站的支持页面中提交支持请求，并附加输出文件。

收集 View Agent、View Client 或 View Connection Server 的诊断信息

如果您能够直接访问控制台，可以使用支持脚本为 View Connection Server、View Client 或运行 View Agent 的桌面生成日志文件。这些信息有助于 VMware 技术支持部门诊断这些组件出现的问题。

前提条件

登录到您希望收集信息的系统。

- 对于 View Agent，请登录安装有 View Agent 的虚拟机。
- 对于 View Client，请登录安装有 View Client 的系统。
- 对于 View Connection Server，请登录 View Connection Server 主机。

步骤

1 打开一个命令提示符窗口，转到您希望收集诊断信息的 VMware View 组件的相应目录。

选项	描述
View Agent	转到 `C:\Program Files\VMware View\Agent\DCT` 目录。
View Client	转到 `C:\Program Files\VMware View\Client\DCT` 目录。
View Connection Server	转到 `C:\Program Files\VMware View\Server\DCT` 目录。

如果您未将软件安装在默认目录中，请替换相应的驱动器盘符和路径。

2 键入命令运行支持脚本。

```
.\support.bat [loglevels]
```

如果您希望启用高级日志记录功能，请指定 `loglevels` 选项并在系统提示时输入日志级别对应的数值。

选项	描述
0	将日志级别重置为默认值。
1	选择常规日志级别（默认）。
2	选择调试日志级别。
3	选择完整日志级别。
4	选择 PCoIP 的信息日志级别（仅适用于 View Agent 和 View Client）。
5	选择 PCoIP 的调试日志级别（仅适用于 View Agent 和 View Client）。
6	选择虚拟通道的信息日志级别（仅适用于 View Agent 和 View Client）。
7	选择虚拟通道的调试日志级别（仅适用于 View Agent 和 View Client）。
8	选择虚拟通道的跟踪日志级别（仅适用于 View Agent 和 View Client）。

脚本会将压缩后的日志文件写入桌面上的 `vdm-sdct` 文件夹。

3 您可以在 `C:\Program Files\Common Files\VMware\View Composer Guest Agent svi-ga-support` 目录下找到 View Composer 客户代理日志。

4 在 VMware 网站的支持页面中提交支持请求，并附加输出文件。

更新支持请求

您可以在支持网站更新现有支持请求。

提交支持请求后，您可能会收到 VMware 技术支持部门发出的电子邮件请求，要求您提供 `support` 或 `svi-support` 脚本的输出文件。运行脚本后，您将看到输出文件的名称和位置。您需要回复电子邮件，并在回复中附加脚本输出文件。

如果输出文件过大（大于或等于 10 MB），请联系 VMware 技术支持部门，告之支持请求编号，请求提供 FTP 上传说明。或者，您也可以在支持网站将输出文件附加到现有支持请求中。

步骤

1 访问并登录 VMware 网站的支持页面。

2 单击 **[Support Request History（支持请求历史记录）]**，查找适当的支持请求编号。

3 更新支持请求，并附加通过运行 `support` 或 `svi-support` 脚本获得的输出文件。

更多故障排除信息

您可以在 VMware 知识库文章中找到更多故障排除信息。

VMware 知识库 (Knowledge Base, KB) 经常更新，以纳入新的 VMware 产品故障排除信息。

有关对 View Manager 进行故障排除的更多信息，请参阅 VMware KB 网站上提供的 KB 文章：

http://kb.vmware.com/selfservice/microsites/microsite.do

排除网络连接问题

您可以采取多种操作来诊断和修复桌面、View Client 和 View Connection Server 实例的网络连接问题。

View Client 与 View Connection Server 之间的连接问题

View Client 与 View Connection Server 之间可能会出现连接问题。

问题

如果 View Client 和 View Connection Server 实例之间出现连接故障，您将看到以下 View Client 错误之一：

- `A secure connection to the server '`*`servername`*`' cannot be established.`（无法与服务器“服务器名”建立安全连接。）
- `The View Connection Server connection failed.`（View Connection Server 连接失败。）

与 View Connection Server 实例进行联系并获取可用桌面列表后，打开桌面也可能会失败。

原因

有很多原因可导致 View Client 与 View Connection Server 实例之间出现连接问题。

- View Client 上的网络代理设置或防火墙设置不正确。
- 建立安全连接时查找 View Connection Server 主机的 DNS 名称失败。

解决方案

1 尝试在浏览器中通过 HTTP 或 HTTPS 访问 View Connection Server 实例。

   如果您看不到登录页面，可运用常规的网络故障排除技术解决该问题。

2 在登录页面中输入有效凭据。

   如果您收到有关无法启动安全连接的错误消息，最有可能的原因是 View Client 或代理服务器（若已配置）无法解析 View Connection Server 主机的 DNS 名称。通过创建文件 `C:\Program Files\VMware\VMware View\Server\sslgateway\conf\locked.properties`，可将主机配置为在指引 View Client 打开安全连接时，报告其主机域名全称 (FQDN) 或 IP 地址。该文件必须包含以下内容，其中 *<网络地址>* 是 View Connection Server 主机的 FQDN 或 IP 地址：

   `clientHost=`*<网络地址>*

3 重新启动 View Connection Server 实例。

桌面与 View Connection Server 实例之间的连接问题

桌面与 View Connection Server 实例之间可能会出现连接问题。

问题

如果桌面和 View Connection Server 实例之间出现连接故障，您将在事件数据库中看到以下某个消息。

- `Provisioning error occurred for Machine` *`Machine_Name`*`:Customization error due to no network communication between the View agent and Connection Server`（部署计算机“计算机名”时出现错误：因 View Agent 和 Connection Server 之间不存在网络通信导致自定义错误）
- `Provisioning error occurred on Pool` *`Desktop_ID`* `because of a networking problem with a View Agent`（部署池“桌面 ID”时因 View Agent 存在网络问题而出现错误）
- `Unable to launch from Pool` *`Desktop_ID`* `for user` *`User_Display_Name`*`:Failed to connect to Machine` *`MachineName`* `using` *`Protocol`*（无法从池“桌面 ID”为用户“用户显示名称”启动桌面：无法通过“协议”连接计算机“计算机名”）

原因

有多种原因可导致桌面与 View Connection Server 实例之间出现连接问题。

- 在桌面上查找 View Connection Server 主机的 DNS 名称失败。
- 用于 JMS、RDP 或 AJP13 通信的端口被防火墙规则阻止。
- View Connection Server 主机上的 JMS 路由器发生故障。

解决方案

- 在桌面的命令提示符下，键入 `nslookup` 命令。

  ```
  nslookup <CS FQDN>
  ```

  其中 <*CS_FQDN*> 是 View Connection Server 主机的主机域名全称 (FQDN)。如果该命令未能返回 View Connection Server 主机的 IP 地址，可运用常规的网络故障排除技术来修改 DNS 配置。
- 在桌面的命令提示符中键入 `telnet` 命令，验证 View Agent 与 View Connection Server 主机建立 JMS 通信时使用的 TCP 端口 4001 是否正常。

  ```
  telnet <CS FQDN> 4001
  ```

  如果建立了 `telnet` 连接，说明 JMS 的网络连接正常。
- 如果在 DMZ 中部署了安全服务器，请检验是否已配置内部防火墙异常规则以允许通过 TCP 端口 3389 在安全服务器与桌面虚拟机之间建立 RDP 连接。
- 如果未使用安全连接，请检验防火墙规则是否允许客户端通过 TCP 端口 3389 与桌面虚拟机建立直接的 RDP 连接，或者通过 TCP 端口 4172 和 UDP 端口 4172 与桌面虚拟机建立直接的 PCoIP 连接。
- 检验是否配置了内部防火墙异常规则以允许每个安全服务器通过 TCP 端口 4001 (JMS) 和 TCP 端口 8009 (AJP13)，和与其关联的 View Connection Server 主机建立连接。

为克隆桌面分配的 IP 地址不正确导致的连接问题

您可能无法连接具有静态 IP 地址的克隆桌面。

问题

您无法用 View Client 连接克隆桌面。

原因

克隆桌面被错误地配置为使用静态 IP 地址，而不是通过 DHCP 来获取其 IP 地址。

解决方案

1 确认 vCenter 上的桌面池模板已配置为使用 DHCP 为桌面分配 IP 地址。

2 在 VMware Infrastructure Client 中，手动从桌面池中克隆一个虚拟机，并确认其通过 DHCP 获取正确的 IP 地址。

排除创建桌面池时出现的问题

您可以用多种方法来诊断和修复创建桌面池时出现的问题。

如果找不到自定义规范，创建池操作将失败

如果找不到自定义规范，创建桌面池的操作将失败。

问题

您将无法创建桌面池并在事件数据库中看到以下消息。

`Provisioning error occurred for Machine`*`Machine_Name`*`:Customization failed for Machine`（部署计算机“计算机名”时出现错误：自定义计算机失败）

原因

最有可能造成此问题的原因是，您的权限不足，无法访问自定义规范或创建池。另一个可能的原因是自定义规范已被重命名或删除。

解决方案

- 检验您是否具有足够的权限来访问自定义规范和创建池。
- 如果自定义规范因重命名或删除而不再存在，可选择另一个规范。

因权限问题导致池创建操作失败

如果 ESX 服务器、ESX 群集或数据中心存在权限问题，您将无法创建桌面池。

问题

您无法在 View Administrator 中创建桌面池，因为模板、ESX 服务器、ESX 群集或数据中心无法访问。

原因

有很多原因可导致出现这种问题。

- 您没有创建池所需的适当权限。
- 您没有访问模板所需的适当权限。
- 您没有访问 ESX 服务器、ESX 群集或数据中心所需的适当权限。

解决方案

- 如果 [Template Selection（模板选择）] 屏幕未显示任何可用模板，请确认您有足够的权限来访问模板。
- 确认您有足够的权限来访问 ESX 服务器、ESX 群集或数据中心。
- 确认您有足够的权限来创建池。

因配置问题导致池部署失败

如果模板不可用或虚拟机映像已被移动或删除，部署桌面池的操作就可能失败。

问题

您将无法部署桌面池并在事件数据库中看到以下消息。

`Provisioning error occurred on Pool` *`Desktop_ID`* `because of a configuration problem`（因配置问题导致池“桌面 ID”出现部署错误）

原因

有很多原因可导致出现这种问题。

- 模板无法访问。
- 模板名称已在 vCenter 中更改。
- 模板已被移到 vCenter 中的其他文件夹。
- 虚拟机映像已在 ESX 服务器之间移动或已被删除。

解决方案

- 确认模板可访问。
- 确认为模板指定的名称和文件夹正确无误。
- 如果在 ESX 服务器之间移动了虚拟机映像，请将虚拟机移到正确的 vCenter 文件夹下。
- 如果删除了虚拟机映像，请在 View Administrator 中删除该虚拟机条目并重新创建或还原映像。

由于 View Connection Server 实例无法连接 vCenter 导致池部署失败

如果 Connection Server 无法连接到 vCenter，部署桌面池的操作会失败。

问题

您将无法部署桌面池并在事件数据库中看到以下某个错误消息。

- `Cannot log in to vCenter at address` *`VC_Address`*（无法登录以 "VC_Address" 为地址的 vCenter）
- `The status of vCenter at address` *`VC_Address`* `is unknown`（以 "VC_Address" 为地址的 vCenter 的状态未知）

原因

导致 View Connection Server 实例无法连接 vCenter 的原因如下。

- vCenter Server 上的 Web 服务已停止。
- View Connection Server 主机与 vCenter Server 之间存在网络连接问题。
- vCenter 或 View Composer 的端口号及详细登录信息已更改。

解决方案

- 确认 vCenter 上正在运行 Web 服务。
- 确认 View Connection Server 主机与 vCenter 之间不存在网络连接问题。
- 在 View Administrator 中，确认为 vCenter 和 View Composer 配置了端口号和详细登录信息。

因数据存储问题导致池部署失败

如果数据存储的磁盘空间不足，或者您的权限不足以访问数据存储，部署桌面池的操作就会失败。

问题

您将无法部署桌面池并在事件数据库中看到以下某个错误消息。

- `Provisioning error occurred for Machine` *`Machine_Name`*`:Cloning failed for Machine`（部署计算机“计算机名”时出现错误：克隆计算机失败）
- `Provisioning error occurred on Pool` *`Desktop_ID`* `because available free disk space is reserved for linked clones`（可用磁盘空间已预留给链接克隆，因此在部署池“桌面 ID” 时出现错误）
- `Provisioning error occurred on Pool` *`Desktop_ID`* `because of a resource problem`（因资源问题导致池“桌面 ID”出现部署错误）

原因

您的权限不足，无法访问所选的数据存储，或者该桌面池的数据存储空间不足。

解决方案

- 确认您有足够的权限来访问所选的数据存储。
- 检验配置了数据存储的磁盘空间是否已满。
- 如果磁盘已满或空间已被预留，请释放一些磁盘空间，重新平衡可用的数据存储，或者将数据存储迁移到较大的磁盘上。

vCenter 过载导致池部署失败

如果 vCenter 由于请求过多而过载，部署桌面池的操作可能会失败。

问题

您将无法部署桌面池并在事件数据库中看到以下错误消息。

`Provisioning error occurred on Pool` *`Desktop_ID`* `because of a timeout while customizing`（因自定义超时导致池“桌面 ID”出现部署错误）

原因

vCenter 由于请求过多而过载。

解决方案

- 降低 vCenter 的部署和电源操作限制。
- 减少 vCenter 允许的并发操作数。
- 配置额外的 vCenter Server。

  有关配置 vCenter 的更多信息，请参阅*《VMware View 安装指南》*。

虚拟机长时间处于“部署”状态

克隆完成后，虚拟机长时间处于 [Provisioning（部署）] 状态。

问题

虚拟机长时间处于 [Provisioning（部署）] 状态。

原因

最有可能造成此问题的原因是，您在克隆操作期间重新启动了 View Connection Server 实例。

解决方案

◆ 删除虚拟机，重新进行克隆。

虚拟机长时间处于“正在自定义”状态

克隆完成后，虚拟机长时间处于 [Customizing（正在自定义）] 状态。

问题

虚拟机长时间处于“自定义”状态。

原因

最有可能造成此问题的原因是，磁盘空间不足，无法启动虚拟机。必须先启动虚拟机，才能进行自定义。

解决方案

- 删除虚拟机，以便从长时间自定义状态中恢复。
- 如果磁盘已满，请释放一些磁盘空间，或者将数据存储迁移到较大的磁盘上。

排除 USB 重定向故障

在 View Client 中进行 USB 重定向时可能会出现各种问题。

问题

View Client 中的 USB 重定向功能无法为远程桌面启用本地设备，或是某些设备看上去无法用于 View Client 重定向。

原因

以下是可能造成 USB 重定向无法正确或按照预期运行的原因。

- Windows 2000 系统或 Microsoft 终端服务管理的 View 桌面不支持 USB 重定向。
- 引导设备不支持 USB 重定向。如果您在通过 USB 设备引导的 Windows 系统上运行 View Client，而且将该设备重定向到远程桌面，本地操作系统就可能无法响应或不可用。请参阅 http://kb.vmware.com/kb/1021409。
- 默认情况下，适用于 Windows 的 View Client 不允许选择人机界面设备 (HID) 以及与之配对的蓝牙设备进行重定向。请参阅http://kb.vmware.com/kb/1011600。
- RDP 不支持用于控制台会话的 USB HID 或智能卡读卡器的重定向。请参阅 http://kb.vmware.com/kb/1011600。
- 使用 USB 闪存卡时，RDP 会导致出现异常问题。请参阅http://kb.vmware.com/kb/1019547。
- Windows Mobile 设备中心可阻止 RDP 会话中的 USB 设备重定向。请参阅 http://kb.vmware.com/kb/1019205。
- 对于某些 USB HID，您必须配置虚拟机来更新鼠标指针的位置。请参阅 http://kb.vmware.com/kb/1022076。
- 某些音频设备可能需要对策略设置或注册表设置进行更改。请参阅http://kb.vmware.com/kb/1023868。
- 网络延迟可能造成设备交互缓慢，或导致应用程序因与本地设备交互而表现为冻结。大型 USB 磁盘驱动器可能需要几分钟才会显示在 Windows 资源管理器中。
- 使用 FAT32 文件系统格式化的 USB 闪存卡加载速度很慢。请参阅http://kb.vmware.com/kb/1022836。

- 本地系统中的进程或服务在您连接远程桌面前打开了设备。
- 如果您重新连接桌面会话，即使桌面显示该设备可用，重定向的 USB 设备也会停止工作。
- 在 View Administrator 中禁用了 USB 重定向。
- 客户机上缺少或禁用了 USB 重定向驱动程序。
- 客户端上缺少或禁用了 USB 重定向驱动程序，或者缺少或禁用了被重定向设备的驱动程序。

.

解决方案

- 如果可能，请使用 PCoIP 代替 RDP 作为桌面协议。
- 如果临时断开连接后重定向的设备仍然不可用或停止工作，则需要拔出并重新插入该设备，然后重新尝试重定向。
- 在 View Administrator 中，进入 **[Policies（策略）] > [Global Policies（全局策略）]**，确定 [View Policies（View 策略）] 下的 USB 访问已被设置为 **[Allow（允许）]**。
- 检查客户机日志中的 `wssm_usb` 分类条目，以及客户端日志中的 `wswc_usb` 分类条目。

  如果用户不是管理员，或者 USB 重定向驱动程序未安装或不能正常运行，这些分类的条目将被写入日志中。
- 打开客户机上的 [Device Manager（设备管理器）]，展开 [Universal Serial Bus controllers（通用串行总线控制器）]，重新安装（如已丢失）或启用（如被禁用）VMware VDM Virtual USB Device Manager 和 VMware VDM Virtual USB Hub 驱动程序。
- 打开客户端上的 [Device Manager（设备管理器）]，展开 [Universal Serial Bus controllers（通用串行总线控制器）]，重新为重定向的设备安装（如已丢失）或启用（如被禁用）VMware VDM Virtual USB Client Device Manager 和 USB 驱动程序。

排除 QuickPrep 自定义问题

造成 View Composer QuickPrep 自定义脚本故障的原因有很多。

问题

QuickPrep 同步后脚本或关机脚本无法执行。在某些情况下，脚本可能只会在一些链接克隆上成功执行，在另外一些上失败。

原因

导致 QuickPrep 脚本故障的常见原因包括：

- 脚本超时
- 脚本路径引用了一个需要使用解释程序的脚本
- 脚本运行时所用的帐户没有足够的权限来执行脚本任务

解决方案

- 查看自定义脚本日志。

  QuickPrep 自定义信息被写入到 Windows `temp` 目录下的日志文件中：

  ```
  C:\Windows\Temp\vmware-viewcomposer-ga-new.log
  ```

- 确定脚本是否超时。

  View Composer 会终止用时超过 20 秒的自定义脚本。日志文件会显示一条提示脚本已经启动的消息，之后还会显示一条超时消息：

  ```
  2010-02-21 21:05:47,687 [1500] INFO Ready -
  [Ready.cpp, 102] Running the PostSync script:cmd /c
  C:\temp\build\composer.bat
  2010-02-21 21:06:07,348 [1500] FATAL Guest -
  [Guest.cpp, 428] script cmd /c
  C:\temp\build\composer.bat timed out
  ```

  要解决此超时问题，请提高脚本的超时限制值并重新运行脚本。

- 确定脚本路径是否有效。

  如果您使用需要解释程序才能执行脚本的脚本语言，则脚本路径必须以解释程序二进制文件的路径为开头。

  例如，如果您指定 `C:\script\myvb.vbs` 作为 QuickPrep 自定义脚本的路径，View Composer Agent 将无法执行该脚本。您必须指定一个以解释程序二进制文件路径开始的路径：

  ```
  C:\windows\system32\cscript.exe c:\script\myvb.vbs
  ```

- 确定用于运行脚本的帐户是否具有合适的权限来执行脚本任务。

  QuickPrep 在配置运行 View Composer Agent 的帐户下运行脚本。默认情况下，这个帐户为 `SYSTEM`。

  您可以使用 Windows 服务 (`services.msc`) 对话框更改 VMware View Composer Guest Agent Server 服务的登录属性，从而更改默认帐户。内部服务名称为 `vmware-viewcomposer-ga`。

View Composer 部署错误

如果 View Composer 部署或重构链接克隆桌面时发生错误，错误代码可指明发生故障的原因。错误代码显示在 View Administrator 中的桌面状态栏中。

表 15-2 介绍了 View Composer 部署错误代码。

此表列出了与 View Composer 和 QuickPrep 自定义相关的错误。View Connection Server 和其他 View 组件中可能还会发生其他干扰桌面部署的错误。

表 15-2 View Composer 部署错误

错误	描述
0	策略已成功应用。 **注意** 结果代码 0 不会出现在 View Administrator 中。除非 View Composer 域外部发生 View Manager 错误，否则链接克隆桌面将进入 [Ready（就绪）] 状态。此结果代码用于表示完整性。
1	未能设置计算机名称。
2	未能将用户配置文件重定向到 View Composer 永久磁盘。
3	未能设置计算机的域帐户密码。
4	未能备份用户配置文件密钥。进行重构操作后，当用户下次登录该链接克隆桌面时，操作系统会为其创建一个新的配置文件目录。创建新的配置文件后，用户将看不到旧的配置文件数据。
5	未能还原用户的配置文件。在此情况下，用户不应登录桌面，因为配置文件的状态还没有定义。

表 15–2 View Composer 部署错误（续）

错误	描述
6	其他错误代码未涵盖的错误。客户操作系统中的 View Composer Agent 日志文件可提供有关这些错误原因的详细信息。 例如，Windows Plug and Play (PnP) 服务超时会生成此错误代码。在此情况下，等待 PnP 服务为链接克隆虚拟机安装新卷之后，View Composer 将会超时。 根据池的配置方式，PnP 最多可以装载三个磁盘： ■ View Composer 永久磁盘 ■ 用于重定向客户操作系统临时文件和页面文件的非永久磁盘 ■ 存储 QuickPrep 配置数据和其他操作系统相关数据的内部磁盘。此磁盘始终与链接克隆一起配置。 超时长度为 10 分钟。如果 PnP 在 10 分钟内未完成磁盘装载，View Composer 将出现故障，并显示错误代码 6。
7	附加到链接克隆的 View Composer 永久磁盘过多。一个克隆最多可以具有三个 View Composer 永久磁盘。
8	某个永久磁盘无法装载到创建池时选定的数据存储。
9	View Composer 无法将一次性数据文件重定向到非永久磁盘。页面文件或临时文件目录没有被重定向。
10	View Composer 在指定的内部磁盘上找不到 QuickPrep 配置策略文件。
12	View Composer 找不到包含 QuickPrep 配置策略文件和其他操作系统相关数据的内部磁盘。
13	不只一个永久磁盘被配置为重定向 Windows 用户配置文件。
14	View Composer 卸载内部磁盘失败。
15	首次启动链接克隆后，View Composer 从配置策略文件中读取的计算机名称与当前系统名称不符。
16	由于客户操作系统的批量许可证未激活，因此 View Composer Agent 没有启动。
17	View Composer Agent 未启动。代理在等待 Sysprep 启动时超时。
18	View Composer Agent 在自定义期间未能将链接克隆虚拟机加入域中。

Windows XP 链接克隆无法加入域

如果您的 Active Directory 在 Windows Server 2008 系统上运行，Windows XP 链接克隆桌面可能无法加入域。

问题

部署链接克隆桌面时，链接克隆无法加入域。View Administrator 显示 View Composer 部署错误消息。例如：

`5/17/10 3:11:50 PM PDT:View Composer agent initialization state error (18):Failed to join the domain (waited 565 seconds)`（5/17/10 3:11:50 PM PDT：View Composer 代理初始化状态错误 (18)：无法加入域（已等待 565 秒））

原因

如果 Active Directory 在 Windows Server 2008 系统上运行，就可能出现这个问题。Windows Server 2008 只读域控制器 (RODC) 无法向后兼容 Windows XP 虚拟机。

解决方案

1 在 View Composer 日志中查看以下错误消息：

   `0x4f1:The system detected a possible attempt to compromise security.Please ensure that you can contact the server that authenticated you.`（0x4f1：系统检测到一个可能危害系统安全的行为，请确保您可以连接对您进行身份验证的服务器。）

   默认情况下，View Composer 日志文件在 Windows `Temp` 目录下生成：`C:\Windows\Temp\vmware-viewcomposer-ga-new.log`

2 在父虚拟机上，对 Windows XP 应用 Windows Server 2008 RODC 兼容性更新。

   请参阅以下位置的 Microsoft 支持文章 944043：http://support.microsoft.com/kb/944043/en-us.

3 为更新的父虚拟机创建快照。

4 从更新的父虚拟机和快照重构链接克隆桌面。

使用 vdmadmin 命令 16

在 View Connection Server 实例上，您可以使用 vdmadmin 命令行界面执行各种管理任务。

您可以使用 vdmadmin 命令执行那些在 View Administrator 用户界面中无法执行的管理任务，或者执行需要通过脚本自动运行的管理任务。

有关 View Administrator、View cmdlets 和 vdmadmin 所能执行操作的对比，请参阅《*VMware View Integration Guide*》（VMware View 集成指南）。

- 使用 -O 和 -P 选项显示未授权用户的桌面和策略第 282 页，

  您可以使用 vdmadmin 命令以及 -O 和 -P 选项显示分配给那些不再具有系统使用授权的用户的桌面和策略。
- 使用 -Q 选项配置 Kiosk 模式客户端第 284 页，

  您可以使用 vdmadmin 命令和 -Q 选项为处于 Kiosk 模式的客户端设置默认值及创建帐户，以及启用这些客户端的身份验证并显示其配置信息。
- 使用 -R 选项显示桌面的首个用户第 287 页，

  您可以使用 vdmadmin 命令和 -R 选项查明受管理桌面的初始分配情况。例如，在丢失 LDAP 数据的情形下，您可能需要此信息，以便重新为用户分配桌面。
- 使用 -S 选项移除 View Connection Server 实例条目第 287 页，

  您可以使用 vdmadmin 命令和 -S 选项从 View Manager 配置中移除 View Connection Server 实例条目。
- 使用 -T 选项设置发布 View Transfer Server 文件包的拆分限制第 288 页，

  您可以使用 vdmadmin 命令和 -T 选项设置发布 View Transfer Server 文件包的拆分限制。如果您使用一个定义了最大缓存目标大小的代理缓存，您可能需要指定拆分限制。
- 使用 -U 选项显示用户信息第 288 页，

  您可以使用 vdmadmin 命令和 -U 选项显示用户的详细信息。
- 使用 -V 选项解密本地桌面的虚拟机第 289 页，

  VMware View 通过对虚拟机的基础映像进行加密来保护本地桌面的虚拟机。如果无法启动或检入本地桌面，您可以将 vdmadmin 命令与 -V 选项配合使用对虚拟机进行解密，以便从中恢复数据。
- 使用 -V 选项解锁或锁定虚拟机第 290 页，

  您可以使用 vdmadmin 命令和 -V 选项解锁或锁定数据中心的虚拟机。

vdmadmin 命令用法

vdmadmin 命令的语法用于控制其操作。

在 Windows 命令提示符下，使用以下 vdmadmin 命令格式。

vdmadmin *<命令选项>* [*<附加选项>* *<自变量>*] ...

您可以使用的附加选项取决于命令选项。

默认情况下，vdmadmin 命令可执行文件的路径为 C:\Program Files\VMware\VMware View\Server\tools\bin。为避免在命令行中输入此路径，可以将此路径添加到 *PATH* 环境变量中。

- vdmadmin 命令身份验证第 268 页，

  为了成功运行指定操作，您必须以 **Administrators** 角色运行 vdmadmin 命令。
- vdmadmin 命令输出格式第 269 页，

  您可以使用某些 vdmadmin 命令选项指定输出信息的格式。
- vdmadmin 命令选项第 269 页，

  您可以使用 vdmadmin 命令的选项来指定该命令执行的操作。

vdmadmin 命令身份验证

为了成功运行指定操作，您必须以 **Administrators** 角色运行 vdmadmin 命令。

您可以用 View Administrator 将 **Administrators** 角色分配给用户。请参阅第 21 页，第 2 章“配置基于角色的委托管理”。

如果您使用权限不足的用户身份登录，则可以使用 `-b` 选项以分配有 **Administrators** 角色的用户身份运行该命令，前提是您知道用户密码。您可以指定 `-b` 选项，作为指定域的指定用户运行 `vdmadmin` 命令。下列形式的 `-b` 选项具有相同的效果。

`-b` *<用户名>* *<域>* `[`*<密码>* `| *]`

`-b` *<用户名>*`@`*<域>* `[`*<密码>* `| *]`

`-b` *<域>*`\`*<用户名>* `[`*<密码>* `| *]`

如果您指定星号 (*) 而非密码，系统会提示您输入密码。`-b` 选项可以与除 `-R` 和 `-T` 选项以外的所有命令选项一起使用。

vdmadmin 命令输出格式

您可以使用某些 `vdmadmin` 命令选项指定输出信息的格式。

表 16-1 显示了某些 `vdmadmin` 命令选项为设置输出文本格式提供的选项。

表 16-1 选择输出格式的选项

选项	描述
`-csv`	将输出格式设置为逗号分隔值格式。
`-n`	用 ASCII (UTF-8) 字符显示输出内容。这是逗号分隔值和纯文本格式输出的默认字符集。
`-w`	用 Unicode (UTF-16) 字符显示输出内容。这是 XML 输出的默认字符集。
`-xml`	以 XML 格式显示输出内容。

vdmadmin 命令选项

您可以使用 `vdmadmin` 命令的选项来指定该命令执行的操作。

表 16-2 显示了可与 `vdmadmin` 命令配合使用以控制和检验 View Manager 运行过程的命令选项。

表 16-2 vdmadmin 命令选项

选项	描述
`-A`	管理 View Agent 记录在其日志文件中的信息。请参阅第 270 页，“使用 -A 选项配置 View Agent 日志”。 覆盖 View Agent 所报告的 IP 地址。请参阅第 271 页，“使用 -A 选项覆盖 IP 地址”
`-C`	为 View Connection Server 组设置名称。请参阅第 272 页，“使用 -C 选项设置 View Connection Server 组名”。
`-F`	为所有用户或指定用户更新 Active Directory 中的外部安全主体 (Foreign Security Principals, FSP)。请参阅第 273 页，“使用 -F 选项更新外部安全主体”。
`-H`	显示 View Manager 服务的运行状况信息。请参阅第 274 页，“使用 -H 选项列出并显示运行状况监视器”。
`-I`	生成关于 View Manager 运行情况的报告。请参阅第 275 页，“使用 -I 选项列出并显示 View Manager 运行报告”。
`-L`	为用户分配专用桌面或者删除所做的分配。请参阅第 275 页，“使用 -L 选项分配专用桌面”。
`-M`	显示关于某个虚拟机或物理机的信息。请参阅第 276 页，“使用 -M 选项显示计算机信息”。
`-N`	配置 View Connection Server 实例或组为 View Client 提供的域。请参阅第 277 页，“使用 -N 选项配置域过滤器”。
`-O`	显示已分配给用户，但用户已不再具有其授权的桌面。请参阅第 282 页，“使用 -O 和 -P 选项显示未授权用户的桌面和策略”。
`-P`	显示与未授权用户的桌面相关联的用户策略。请参阅第 282 页，“使用 -O 和 -P 选项显示未授权用户的桌面和策略”。

表 16–2 vdmadmin 命令选项 （续）

选项	描述
-Q	在 Active Directory 帐户中配置帐户以及处于 kiosk 模式的客户端设备的 View Manager 配置。请参阅第 284 页，“使用 -Q 选项配置 Kiosk 模式客户端”。
-R	报告第一个访问桌面的用户。请参阅第 287 页，“使用 -R 选项显示桌面的首个用户”。
-S	从 View Manager 的配置中移除一个针对 View Connection Server 实例的配置条目。请参阅第 287 页，“使用 -S 选项移除 View Connection Server 实例条目”。
-T	为 View Transfer Server 程序包设置拆分限制。请参阅第 288 页，“使用 -T 选项设置发布 View Transfer Server 文件包的拆分限制”。
-U	显示关于用户的信息，包括他们的桌面授权和 ThinApp 分配，以及 Administrator 角色。请参阅第 288 页，“使用 -U 选项显示用户信息”。
-V	允许通过解密其虚拟机从本地桌面恢复数据。请参阅第 289 页，“使用 -V 选项解密本地桌面的虚拟机”。 解锁或锁定虚拟机，其中包括本地桌面和 View Transfer Server 实例。请参阅第 290 页，“使用 -V 选项解锁或锁定虚拟机”。

使用 -A 选项配置 View Agent 日志

您可以使用 `vdmadmin` 命令和 -A 选项配置 View Agent 生成的日志。

语法

```
vdmadmin -A [-b <身份验证自变量>] -getDCT -outfile <本地文件> -d <桌面> -m <计算机>

vdmadmin -A [-b <身份验证自变量>>] -getlogfile <日志文件> -outfile <本地文件> -d <桌面> -m <计算机>

vdmadmin -A [-b <身份验证自变量>] -getloglevel [-xml] -d <桌面> [-m <计算机>]

vdmadmin -A [-b <身份验证自变量>] -getstatus [-xml] -d <桌面> [-m <计算机>]

vdmadmin -A [-b <身份验证自变量>] -getversion [-xml] -d <桌面> [-m <计算机>]

vdmadmin -A [-b <身份验证自变量>] -list [-xml] [-w | -n] -d <桌面> -m <计算机>

vdmadmin -A [-b <身份验证自变量>] -setloglevel <级别> -d <桌面> [-m <计算机>]
```

用法说明

为了协助 VMware 技术支持部门排除 View Agent 故障，您可以创建一个数据收集工具 (Data Collection Tool, DCT) 捆绑包。您还可以更改日志级别、显示 View Agent 的版本和状态以及在本地磁盘上保存独立的日志文件。

选项

表 16–3 列出了配置 View Agent 日志时您可以指定的选项。

表 16–3 在 View Agent 中配置日志的选项

选项	描述
`-d` *<桌面>*	指定桌面池。
`-getDCT`	创建一个数据收集工具 (Data Collection Tool, DCT) 捆绑包并将其保存在本地文件中。
`-getlogfile` *<日志文件>*	指定要保存副本的日志文件的名称。
`-getloglevel`	显示 View Agent 当前的日志级别。
`-getstatus`	显示 View Agent 状态。
`-getversion`	显示 View Agent 版本。

表 16–3 在 View Agent 中配置日志的选项 （续）

选项	描述	
`-list`	列出 View Agent 的日志文件。	
`-m` <*计算机*>	指定桌面池中的计算机。	
`-outfile` <*本地文件*>	指定要保存 DCT 捆绑包或日志文件副本的本地文件的名称。	
`-setloglevel` <*级别*>	设置 View Agent 的日志级别。	
	debug	记录错误、警告和调试事件。
	normal	记录错误和警告事件。
	trace	记录错误、警告、信息和调试事件。

示例

显示桌面池 dtpool2 中虚拟机 machine1 的 Agent 日志级别。

```
vdmadmin -A -d dtpool2 -m machine1 -getloglevel
```

将桌面池 dtpool2 中虚拟机 machine1 的 View Agent 的日志级别设为 debug。

```
vdmadmin -A -d dtpool2 -m machine1 -setloglevel debug
```

显示桌面池 dtpool2 中虚拟机 machine1 的 View Agent 日志文件列表。

```
vdmadmin -A -d dtpool2 -m machine1 -list
```

将桌面池 dtpool2 中虚拟机 machine1 的 View Agent 日志文件 `log-2009-01-02.txt` 另存为副本 `C:\mycopiedlog.txt`。

```
vdmadmin -A -d dtpool2 -m machine1 -getlogfile log-2009-01-02.txt -outfile C:\mycopiedlog.txt
```

显示桌面池 dtpool2 中虚拟机 machine1 的 View Agent 版本。

```
vdmadmin -A -d dtpool2 -m machine1 -getversion
```

显示桌面池 dtpool2 中虚拟机 machine1 的 View Agent 状态。

```
vdmadmin -A -d dtpool2 -m machine1 -getstatus
```

为桌面池 dtpool2 中的虚拟机 machine1 创建 DCT 捆绑包，并将其写入 zip 文件 `C:\myfile.zip` 中。

```
vdmadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

使用 -A 选项覆盖 IP 地址

您可以使用 `vdmadmin` 命令和 -A 选项覆盖 View Agent 所报告的 IP 地址。

语法

```
vdmadmin -A [-b <身份验证自变量>] -override -i <IP 或 DNS> -d <桌面> -m <计算机>
vdmadmin -A [-b <身份验证自变量>] -override -list -d <桌面> -m <计算机>
vdmadmin -A [-b <身份验证自变量>] -override -r -d <桌面> [-m <计算机>]
```

用法说明

View Agent 可找出运行它的虚拟机的 IP 地址并报告给 View Connection Server 实例。在安全性较高的配置中，View Connection Server 实例不会信任 View Agent 所报告的值，您可以覆盖由 View Agent 提供的值，并指定受管虚拟机应采用的 IP 地址。如果 View Agent 报告的虚拟机地址与所定义的地址不符，您就无法通过 View Client 访问该虚拟机。

选项

表 16-4 列出了覆盖 IP 地址时您可以指定的选项。

表 16–4 覆盖 IP 地址的选项

选项	描述
`-d` <*桌面*>	指定桌面池。
`-i`<*IP 或 DNS*>	指定 IP 地址或 DNS 中可解析的域名。
`-m` <*计算机*>	指定桌面池中虚拟机的名称。
`-override`	指定一个覆盖 IP 地址的操作。
`-r`	移除被覆盖的 IP 地址。

示例

覆盖桌面池 dtpool2 中虚拟机 machine2 的 IP 地址。

```
vdmadmin -A -override -i 10.20.54.165 -d dtpool2 -m machine2
```

显示为桌面池 dtpool2 中的虚拟机 machine2 定义的 IP 地址。

```
vdmadmin -A -override -list -d dtpool2 -m machine2
```

移除为桌面池 dtpool2 中虚拟机 machine2 定义的 IP 地址。

```
vdmadmin -A -override -r -d dtpool2 -m machine2
```

移除为桌面池 dtpool3 中的桌面定义的 IP 地址。

```
vdmadmin -A -override -r -d dtpool3
```

使用 -C 选项设置 View Connection Server 组名

您可以使用 `vdmadmin` 命令和 `-C` 选项设置 View Connection Server 组的名称。Microsoft System Center Operations Manager (SCOM) 控制台将显示该名称，以帮助您在 SCOM 内识别该组。

语法

```
vdmadmin -C [-b <身份验证自变量>] [-c <组名>]
```

用法说明

如果您要使用 SCOM 监视和管理 View Manager 组件的状态，就必须为 View Connection Server 组命名。View Administrator 不会显示组名。在您想要命名的组的某个成员上运行此命令。

如果您没有为组指定名称，此命令将会返回本地 View Connection Server 实例所属组的 GUID。您可以使用此 GUID 来验证一个 View Connection Server 实例是否与另一个 View Connection Server 实例属于同一 View Connection Server 组。

关于如何将 SCOM 与 VMware View 结合使用的说明，请参阅《*VMware View Integration Guide*》（VMware View 集成指南）。

选项

`-c` 选项可指定 View Connection Server 组名。如果您没有指定此选项，该命令会返回组 GUID。

示例

将 View Connection Server 组的名称设置为 VCSG01。

```
vdmadmin -C -c VCSG01
```

返回组 GUID。

```
vdmadmin -C
```

使用 -F 选项更新外部安全主体

您可以使用 `vdmadmin` 命令和 `-F` 选项更新 Active Directory 中有权使用桌面的 Windows 用户的外部安全主体 (Foreign Security Principal, FSP)。

语法

```
vdmadmin -F [-b <身份验证自变量>] [-u 域\用户]
```

用法说明

如果您信任本地域以外的域，就会允许外部域中的安全主体访问本地域的资源。Active Directory 用 FSP 来代表受信任的外部域中的安全主体。如果您修改受信任的外部域列表，则可能需要更新用户的 FSP。

选项

`-u` 选项可指定您希望更新 FSP 的用户的名称和域。如果您没有指定此选项，该命令会更新 Active Directory 中所有用户的 FSP。

示例

更新域 EXTERNAL 中用户 Jim 的 FSP。

```
vdmadmin -F -u EXTERNAL\Jim
```

更新 Active Directory 中所有用户的 FSP。

```
vdmadmin -F
```

使用 -H 选项列出并显示运行状况监视器

您可以使用 `vdmadmin` 命令 -H 列出现有的运行状况监视器，对 View Manager 组件的实例进行监视，并显示特定运行状况监视器或监视器实例的详细信息。

语法

```
vdmadmin -H [-b <身份验证自变量>] -list -xml [-w | -n]

vdmadmin -H [-b <身份验证自变量>] -list -monitorid <监视器 ID> -xml [-w | -n]

vdmadmin -H [-b <身份验证自变量>] -monitorid <监视器 ID> -instanceid <实例 ID> -xml [-w | -n]
```

用法说明

表 16-5 显示了 View Manager 用来监视其组件运行状况的运行状况监视器。

表 16–5 运行状况监视器

监视器	描述
CBMonitor	监视 View Connection Server 实例的运行状况。
DBMonitor	监视事件数据库的运行状况。
DomainMonitor	监视 View Connection Server 主机的本地域及所有信任域的运行状况。
SGMonitor	监视安全网关服务和安全服务器的运行状况。
TSMonitor	监视传输服务器的运行状况。
VCMonitor	监视 vCenter 服务器的运行状况。

如果某个组件具有若干实例，View Manager 会创建单独的监视器实例来监视该组件的每个实例。

此命令会以 XML 格式输出关于运行状况监视器和监视器实例的所有信息。

选项

表 16–6 列出了您要列出并显示运行状况监视器时可以指定的选项。

表 16–6 列出并显示运行状况监视器的选项

选项	描述
`-instanceid` <*实例 ID*>	指定一个运行状况监视器实例
`-list`	如果未指定运行状况监视器 ID，则显示现有的运行状况监视器。
`-list -monitorid` <*监视器 ID*>	显示指定运行状况监视器 ID 的监视器实例。
`-monitorid` <*监视器 ID*>	指定一个运行状况监视器 ID。

示例

以 XML 格式（使用 Unicode 字符）列出现有的所有运行状况监视器。

```
vdmadmin -H -list -xml
```

以 XML 格式（使用 ASCII 字符）列出 vCenter 监视器 (VCMonitor) 的所有实例。

```
vdmadmin -H -list -monitorid VCMonitor -xml -n
```

显示指定 vCenter 监视器实例的运行状况。

```
vdmadmin -H -monitorid VCMonitor -instanceid 4aec2c99-4879-96b2-de408064d035 -xml
```

使用 -I 选项列出并显示 View Manager 运行报告

您可以使用 `vdmadmin` 命令和 `-I` 选项列出可用的 View Manager 运行报告，并显示运行这些报告的结果。

语法

```
vdmadmin -I [-b <身份验证自变量>] -list [-xml] [-w | -n]
```

```
vdmadmin -I [-b <身份验证自变量>] -report <报告> -view <视图> [-startdate yyyy-MM-dd-HH:mm:ss]
[-enddate yyyy-MM-dd-HH:mm:ss] [-w | -n] -xml | -csv
```

用法说明

您可以用此命令显示可用的报告和视图，并显示 View Manager 为指定报告和视图记录的信息。

选项

表 16-7 列出了您在列出并显示报告和视图时可以指定的选项。

表 16–7 列出并显示报告和视图的选项

选项	描述
`-enddate` *yyyy-MM-dd-HH:mm:ss*	指定显示信息的日期上限。
`-list`	列出可用的报告和视图。
`-report` *<报告>*	指定一个报告。
`-startdate` *yyyy-MM-dd-HH:mm:ss*	指定显示信息的日期下限。
`-view` *<视图>*	指定一个视图。

示例

以 XML 格式（使用 Unicode 字符）列出可用的报告和视图。

```
vdmadmin -I -list -xml -w
```

以逗号分隔值格式（使用 ASCII 字符）显示自 2010 年 8 月 1 日以来发生的用户事件列表。

```
vdmadmin -I -report events -view user_events -startdate 2010-08-01-00:00:00 -csv -n
```

使用 -L 选项分配专用桌面

您可以使用 `vdmadmin` 命令和 `-L` 选项从一个专用池中向用户分配桌面。

语法

```
vdmadmin -L [-b <身份验证自变量>] -d <桌面> -m <计算机> -u <域>\<用户>
```

```
vdmadmin -L[-b <身份验证自变量>] -d <桌面> [-m <计算机> | -u <域>\<用户>] -r
```

用法说明

用户第一次连接到专用桌面池时，View Manager 会给用户分配桌面。在某些情况下，您可能需要为用户预分配桌面。例如，您可能需要在他们初次连接前准备好系统环境。当用户连接到 View Manager 从专用池分配的桌面后，在桌面源的使用期限内，此桌面将始终分配给该用户。您可以将用户分配到专用池中的单个虚拟机。

您可以将桌面分配给任何经授权的用户。当您要恢复 View Connection Server 实例上丢失的 View LDAP 数据，或者要更改特定桌面源的所有权时，可能需要执行此操作。

当用户连接到 View Manager 从专用池分配的桌面后，在桌面源的使用期限内，此桌面将始终分配给该用户。对于离开组织的用户、无需再访问桌面的用户或使用另一桌面池中桌面的用户，您可能需要移除这些用户的桌面分配。您还可以移除对访问桌面池的所有用户分配。

选项

表 16-8 列出了您为用户分配桌面或移除分配时可以指定的选项。

表 16–8 分配专用桌面的选项

选项	描述
-d <*桌面*>	指定桌面池名称。
-m <*计算机*>	指定虚拟机名称。
-r	移除授予指定用户的分配，或移除指定计算机上的所有分配。
-u <*域*>\<*用户*>	指定用户的登录名和域。

示例

将桌面池 dtpool1 中的虚拟机 machine2 分配给域 CORP 中的用户 Jo。

```
vdmadmin -L -d dtpool1 -m machine2 -u CORP\Jo
```

移除桌面池 dtpool1 中对 CORP 域用户 Jo 的桌面分配。

```
vdmadmin -L -d dtpool1 -u Corp\Jo -r
```

移除对桌面池 dtpool3 中计算机 machine1 的所有用户分配。

```
vdmadmin -L -d dtpool3 -m machine1 -r
```

使用 -M 选项显示计算机信息

您可以使用 `vdmadmin` 命令和 -M 选项显示虚拟机或物理机的配置信息。

语法

```
vdmadmin -M [-b <身份验证自变量>] [-m <计算机> | [[-u <域>\<用户>][-d <桌面>]] [-xml | -csv] [-w | -n]
```

用法说明

此命令可显示桌面的底层虚拟机或物理机的相关信息。

- 显示计算机名称。
- 桌面池名称。
- 计算机状态。
- 被分配的用户的 SID。
- 被分配的用户的帐户名。
- 被分配的用户的域名。
- 本地桌面的脱机状态（不适用于 4.0 版或更低版本）。
- 虚拟机的详细目录（如果存在）。
- 虚拟机的创建日期。

- 虚拟机的模板路径（如果存在）。
- vCenter Server 的 URL（如果存在）。

选项

表 16‑9 中的选项可用来指定要显示详细信息的计算机。

表 16‑9 显示计算机信息的选项

选项	描述
-d <*桌面*>	指定桌面池名称。
-m <*计算机*>	指定虚拟机名称。
-u <*域*>\<*用户*>	指定用户的登录名和域。

示例

显示池 dtpool2 中分配给 CORP 域用户 Jo 的桌面的底层计算机相关信息，并将输出格式设为使用 ASCII 字符的 XML 格式。

```
vdmadmin -M -u CORP\Jo -d dtpool2 -xml -n
```

显示计算机 machine3 的相关信息，并将输出格式设为逗号分隔值格式。

```
vdmadmin -M -m machine3 -csv
```

使用 -N 选项配置域过滤器

您可以使用 `vdmadmin` 命令和 `-N` 选项控制 View Manager 允许最终用户访问的域。

语法

```
vdmadmin -N [-b <身份验证自变量>] -domains {-exclude | -include | -search} -domain <域> -add [-s <connsvr>]
```

```
vdmadmin -N [-b <身份验证自变量>] -domains -list [-w | -n] [-xml]
```

```
vdmadmin -N [-b <身份验证自变量>] -domains -list -active [-w | -n] [-xml]
```

```
vdmadmin -N [-b <身份验证自变量>] -domains {-exclude | -include | -search} -domain <域> -remove [-s <connsvr>]
```

```
vdmadmin -N [-b <身份验证自变量>] -domains {-exclude | -include | -search} -removeall [-s <connsvr>]
```

用法说明

指定 `-exclude`、`-include` 或 `-search` 中的一个选项，以将操作分别应用于排除列表、包含列表或搜索排除列表。

如果您将一个域添加到搜索排除列表，该域不会包含在自动域搜索中。

如果您将一个域添加到包含列表，该域会包含在搜索结果中。

如果您将一个域添加到排除列表，该域不会包含在搜索结果中。

选项

表 16‑10 列出了配置域过滤器时您可以指定的选项。

表 16–10 配置域过滤器的选项

选项	描述
-add	将域添加到列表中。
-domain <*域*>	指定要过滤的域。 必须用域的 NetBIOS 名称而非 DNS 名称来指定域。
-domains	指定一个域过滤操作。
-exclude	在排除列表中指定操作。
-include	在包含列表中指定操作。
-list	显示每个 View Connection Server 实例上和用于 View Connection Server 组的搜索排除列表、排除列表以及包含列表中配置的域。
-list -active	显示运行该命令的 View Connection Server 实例上可用的域。
-remove	从列表中移除域。
-removeall	从列表中移除所有域。
-s <*connsvr*>	指定应用于 View Connection Server 实例上域过滤器的操作。您可以按照名称或 IP 地址指定 View Connection Server 实例。 如果不指定该选项，您对搜索配置所做的任何更改都会应用于组中的所有 View Connection Server 实例。
-search	在搜索排除列表中指定操作。

示例

将域 FARDOM 添加到 View Connection Server 实例 csvr1 的搜索排除列表中。

```
vdmadmin -N -domains -search -domain FARDOM -add -s csvr1
```

将域 NEARDOM 添加到 View Connection Server 组的排除列表中。

```
vdmadmin -N -domains -exclude -domain NEARDOM -add
```

显示组中 View Connection Server 实例以及用于组的域搜索配置。

```
C:\ vdmadmin -N -domains -list

Domain Configuration
====================
Cluster Settings
Include:
Exclude:
Search :
FARDOM
DEPTX

Broker Settings:CONSVR-1
Include:
(*)Exclude:
YOURDOM
Search :

Broker Settings:CONSVR-2
Include:
Exclude:
Search :
```

View Manager 会对组中每个 View Connection Server 主机上的域搜索进行限制，以排除 FARDOM 和 DEPTX 域。CONSVR-1 的排除列表旁边的 (*) 字符表示 View Manager 会将 YOURDOM 域从 CONSVR-1 上的域搜索结果列表中排除。

以使用 ASCII 字符的 XML 格式显示域过滤器。

```
vdmadmin -N -domains -list -xml -n
```

显示本地 View Connection Server 实例上当前对 View Manager 可用的域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain:MYDOM

Domain:MYDOM DNS:mydom.mycorp.com
Domain:YOURDOM DNS:yourdom.mycorp.com
Domain:FARDOM DNS:fardom.mycorp.com
Domain:DEPTX DNS:deptx.mycorp.com
Domain:DEPTY DNS:depty.mycorp.com
Domain:DEPTZ DNS:deptz.mycorp.com
```

以使用 ASCII 字符的 XML 格式显示可用的域。

```
vdmadmin -N -domains -list -active -xml -n
```

从 View Connection Server 组的排除列表中移除域 NEARDOM。

```
vdmadmin -N -domains -exclude -domain NEARDOM -remove
```

从 View Connection Server 实例 csvr1 的包含列表中移除所有域。

```
vdmadmin -N -domains -include -removeall -s csvr1
```


配置域过滤器

您可以配置域过滤器以限制 View Connection Server 实例或安全服务器为最终用户提供的域。

View Manager 通过遍历信任关系确定可以访问哪些域，从 View Connection Server 实例或安全服务器所在的域开始。对于一组连接良好的小型域，View Manager 能够快速确定完整的域列表，但随着域数量的不断增多或域之间连通性能的逐渐降低，确定完整域列表所需的时间也会随之增加。View Manager 还可能在搜索结果中包含您不希望在用户登录桌面时为其提供的域。

如果您先前已将控制递归域枚举的 Windows 注册表项 (`HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RecursiveDomainEnum`) 的值设为 false，则会禁用递归域搜索，View Connection Server 实例将仅搜索主域。要使用域过滤功能，需删除该注册表项，或者将其值设为 true，然后重新启动系统。您必须在设置了该注册表项的每个 View Connection Server 实例上执行上述操作。

表 16-11 显示了您可以指定为配置域过滤的域列表类型。

表 16–11 域列表类型

域列表类型	描述
搜索排除列表	指定 View Manager 在自动搜索过程中可以遍历的域。该搜索过程将忽略那些包含在搜索排除列表中的域，并且不会试图定位被排除的域所信任的域。您无法将主域排除在搜索过程以外。
排除列表	指定 View Manager 将从域搜索结果中排除的域。您无法排除主域。
包含列表	指定 View Manager 不从域搜索结果中排除的域。其他所有域（不包括主域）都将被排除。

自动域搜索会检索域列表，排除您在搜索排除列表中指定的域，以及被排除的域所信任的域。View Manager 将按以下顺序选择第一个非空排除列表或包含列表。

1 为 View Connection Server 实例配置的排除列表。

2 为 View Connection Server 组配置的排除列表。

3 为 View Connection Server 实例配置的包含列表。

4 为 View Connection Server 组配置的包含列表。

View Manager 仅应用它选择的第一个列表来生成搜索结果。

如果您指定包含某个域，而该域的控制器当前无法访问，View Manager 将不把该域包含在活动域列表中。

您无法排除 View Connection Server 实例或安全服务器所属的主域。

包含域的过滤操作示例

您可以使用包含列表来指定 View Manager 不从域搜索结果中排除的域。其他所有域（不包括主域）都将被排除。

一个 View Connection Server 实例加入了 MYDOM 主域，并与 YOURDOM 域存在信任关系。YOURDOM 域与 DEPTX 具有信任关系。

对 View Connection Server 实例显示当前活动的域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain:MYDOM

Domain:MYDOM DNS:mydom.mycorp.com
Domain:YOURDOM DNS:yourdom.mycorp.com
Domain:FARDOM DNS:fardom.mycorp.com
Domain:DEPTX DNS:deptx.mycorp.com
Domain:DEPTY DNS:depty.mycorp.com
Domain:DEPTZ DNS:deptz.mycorp.com
```

DEPTY 和 DEPTZ 域出现在列表中，因为它们是 DEPTX 域所信任的域。

指定 View Connection Server 实例应只使 YOURDOM 和 DEPTX 域可用（除了主域 MYDOM 以外）。

```
vdmadmin -N -domains -include -domain YOURDOM -add
vdmadmin -N -domains -include -domain DEPTX -add
```

显示包含 YOURDOM 和 DEPTX 域之后当前活动的域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain:MYDOM
Domain:MYDOM DNS:mydom.mycorp.com
Domain:YOURDOM DNS:yourdom.mycorp.com
Domain:DEPTX DNS:deptx.mycorp.com
```

View Manager 会将该包含列表应用于域搜索结果。如果域层次结构非常复杂，或是与某些域的网络连通性较差，那么域搜索速度可能会较慢。在这种情况下，可改用搜索排除。

排除域的过滤操作示例

您可以使用排除列表来指定 View Manager 将从域搜索结果中排除的域。

一个包含两个 View Connection Server 实例（CONSVR-1 和 CONSVR-2）的组加入到了 MYDOM 主域中，并与 YOURDOM 域存在信任关系。YOURDOM 域与 DEPTX 和 FARDOM 域具有信任关系。

FARDOM 域在远程地理位置，与该域的网络连接速度缓慢且延迟较高。FARDOM 域中的用户不需要访问 MYDOM 域中的 View Connection Server 组。

对 View Connection Server 组中的成员显示当前活动的域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
=============================
Primary Domain:MYDOM

Domain:MYDOM DNS:mydom.mycorp.com
Domain:YOURDOM DNS:yourdom.mycorp.com
Domain:FARDOM DNS:fardom.mycorp.com
Domain:DEPTX DNS:deptx.mycorp.com
Domain:DEPTY DNS:depty.mycorp.com
Domain:DEPTZ DNS:deptz.mycorp.com
```

DEPTY 和 DEPTZ 域是 DEPTX 域所信任的域。

要改进 View 客户端的连接性能，可将 FARDOM 域从 View Connection Server 组的搜索过程中排除。

```
vdmadmin -N -domains -search -domain FARDOM -add
```

此命令可显示将 FARDOM 域从搜索中排除后的活动域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
=============================
Primary Domain:MYDOM

Domain:MYDOM DNS:mydom.mycorp.com
Domain:YOURDOM DNS:yourdom.mycorp.com
Domain:DEPTX DNS:deptx.mycorp.com
Domain:DEPTY DNS:depty.mycorp.com
Domain:DEPTZ DNS:deptz.mycorp.com
```

扩展搜索排除列表，以便将 DEPTX 域及其信任的所有域从组中所有 View Connection Server 实例的域搜索中排除。同时，将 YOURDOM 域排除在 CONSVR-1 可访问的范围以外。

```
vdmadmin -N -domains -search -domain DEPTX -add
vdmadmin -N -domains -exclude -domain YOURDOM -add -s CONSVR-1
```

显示新的域搜索配置。

```
C:\ vdmadmin -N -domains -list

Domain Configuration
====================
Cluster Settings
Include:
Exclude:
```

```
Search :
FARDOM
DEPTX

Broker Settings:CONSVR-1
Include:
(*)Exclude:
YOURDOM
Search :

Broker Settings:CONSVR-2
Include:
Exclude:
Search :
```

View Manager 会对组中每个 View Connection Server 主机上的域搜索进行限制，以排除 FARDOM 和 DEPTX 域。CONSVR-1 的排除列表旁边的 (*) 字符表示 View Manager 会将 YOURDOM 域从 CONSVR-1 上的域搜索结果列表中排除。

在 CONSVR-1 上，显示当前的活动域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
=============================
Primary Domain:MYDOM

Domain:MYDOM DNS:mydom.mycorp.com
```

在 CONSVR-2 上，显示当前的活动域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-2)
=============================
Primary Domain:MYDOM

Domain:MYDOM DNS:mydom.mycorp.com
Domain:YOURDOM DNS:yourdom.mycorp.com
```

使用 -O 和 -P 选项显示未授权用户的桌面和策略

您可以使用 `vdmadmin` 命令以及 `-O` 和 `-P` 选项显示分配给那些不再具有系统使用授权的用户的桌面和策略。

语法

`vdmadmin -O [-b` *<身份验证自变量>*`] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath` *<路径>*`]]`

`vdmadmin -P [-b` *<身份验证自变量>*`] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath` *<路径>*`]]`

用法说明

如果您撤消某个用户对永久桌面或物理系统的权限，并不会自动撤消相关联的桌面分配。如果您临时暂停了用户的帐户，或者用户正在休假，这种情况是可以接受的。当您重新启用授权后，用户可以像以前一样继续使用同一桌面。如果用户离开了组织，其他用户将无法访问该用户的桌面，该桌面会被视为孤立。您可能还希望检查分配给未授权用户的策略。

选项

表 16–12 显示了您在显示未授权用户桌面和策略时可以指定的选项。

表 16–12 显示未授权用户的桌面和策略的选项

选项	描述
`-ld`	按桌面对输出条目排序。
`-lu`	按用户对输出条目排序。
`-noxslt`	指定输出的 XML 文件不应用默认样式表。
`-xsltpath` <*路径*>	指定用于转换 XML 输出的样式表的路径。

表 16–13 显示了可应用于 XML 输出以转换为 HTML 的样式表。该样式表位于 `C:\Program Files\VMware\VMware View\server\etc` 目录下。

表 16–13 XSL 样式表

样式表文件名	描述
`list-checkedout-unentitled.xsl`	转换那些包含未授权用户检出的桌面列表的报告。
`unentitled-machines.xsl`	转换那些包含当前分配给用户的未授权桌面（按用户或系统分组）列表的报告。这是默认的样式表。
`unentitled-policies.xsl`	转换那些包含应用到未授权用户的用户级别策略的桌面列表的报告。

示例

以文本格式显示分配给未授权用户（按桌面分组）的桌面。

```
vdmadmin -O -ld
```

以 XML 格式（使用 ASCII 字符）显示分配给未授权用户（按用户分组）的桌面。

```
vdmadmin -O -lu -xml -n
```

应用您自己的样式表（位于 `C:\tmp\unentitled-users.xsl`），将输出重定向至文件 `uu-output.html`。

```
vdmadmin -O -lu -xml -xsltpath "C:\tmp\unentitled-users.xsl" > uu-output.html
```

以 XML 格式（使用 Unicode 字符）显示与未授权用户的桌面（按桌面分组）相关联的策略。

```
vdmadmin -P -ld -xml -w
```

应用您自己的样式表（位于 `C:\tmp\unentitled-policies.xsl`），将输出重定向至文件 `up-output.html`。

```
vdmadmin -P -ld -xml -xsltpath "C:\tmp\unentitled-policies.xsl" > up-output.html
```

使用 -Q 选项配置 Kiosk 模式客户端

您可以使用 `vdmadmin` 命令和 `-Q` 选项为处于 Kiosk 模式的客户端设置默认值及创建帐户，以及启用这些客户端的身份验证并显示其配置信息。

语法

```
vdmadmin -Q -clientauth -add [-b <身份验证自变量>] -domain <域名> -clientid <客户端 ID> [-password "<密码>" | -genpassword] [-ou <DN>] [-expirepassword | -noexpirepassword] [-group <组名> | -nogroup] [-description "描述文本"]

vdmadmin -Q -disable [-b <身份验证自变量>] -s <连接服务器>

vdmadmin -Q -enable [-b <身份验证自变量>] -s <连接服务器> [-requirepassword]

vdmadmin -Q -clientauth -getdefaults [-b <身份验证自变量>] [-xml]

vdmadmin -Q -clientauth -list [-b <身份验证自变量>] [-xml]

vdmadmin -Q -clientauth -remove [-b <身份验证自变量>] -domain <域名> -clientid <客户端 ID>

vdmadmin -Q -clientauth -removeall [-b <身份验证自变量>] [-force]

vdmadmin -Q -clientauth -setdefaults [-b <身份验证自变量>] [-ou <DN>] [ -expirepassword | -noexpirepassword ] [-group <组名> | -nogroup]

vdmadmin -Q -clientauth -update [-b <身份验证自变量>] -domain <域名> -clientid <客户端 ID> [-password "<密码>" | -genpassword] [-description "描述文本"]
```

用法说明

您必须在客户端用来连接其桌面的 View Connection Server 实例所在组中的一个 View Connection Server 实例运行 `vdmadmin` 命令。

当您为密码到期项和 Active Directory 组成员关系配置默认值时，这些设置会由组中所有的 View Connection Server 实例共享。

添加 kiosk 模式客户端时，View Manager 会在 Active Directory 中为该客户端创建一个用户帐户。如果为客户端指定名称，则该名称必须以字符 "Custom-" 开头，而且名称长度不得超过 20 个字符。每个指定名称只能用于一个客户端设备。如果您没有为客户端指定名称，View Manager 将通过您为客户端设备指定的 MAC 地址生成一个名称。例如，如果 MAC 地址是 00:10:db:ee:76:80，则相应的帐户名是 cm-00_10_db_ee_76_80。您只能在用来对客户端进行身份验证的 View Connection Server 实例中使用这些帐户。

自动生成的密码长度是 16 位，包含至少一个大写字母、一个小写字母、一个符号和一个数字，可以包含重复的字符。如果您需要一个更强的密码，则必须使用 `-password` 选项指定密码。

如果您用 `-group` 选项指定一个组，或者您之前已经设置了默认组，View Manager 会将该客户端的帐户加入该组。您可以指定 `-nogroup` 选项，以免将该帐户加入任何组中。

如果您启用一个 View Connection Server 实例以对 kiosk 模式客户端进行身份验证，您可以指定客户端必须提供密码（可选）。如果您禁用身份验证，客户端将无法连接到其桌面。

即便为单个 View Connection Server 实例启用或禁用身份验证，组中所有的 View Connection Server 实例仍会共享客户端身份验证的所有其他设置。您只需添加一次客户端，组中所有的 View Connection Server 实例都将能够接受来自该客户端的请求。

如果您在启用身份验证时指定 `-requirepassword` 选项，View Connection Server 实例将无法对自动生成密码的客户端进行身份验证。如果您更改 View Connection Server 实例的配置来指定该选项，此类客户端无法对自身进行身份验证，而且会返回错误消息 `Unknown username or bad password`（未知用户名或无效密码）。

选项

表 16-14 列出了配置 kiosk 模式客户端时您可以指定的选项。

表 16–14 配置 kiosk 模式客户端的选项

选项	描述
`-add`	为 kiosk 模式客户端添加一个帐户。
`-clientauth`	指定一个为 kiosk 模式客户端配置身份验证的操作。
`-clientid` <*客户端 ID*>	指定客户端的名称或 MAC 地址。
`-description` "*描述文本*"	在 Active Directory 中为客户端设备创建帐户描述。
`-disable`	在指定 View Connection Server 实例中禁用 kiosk 模式客户端的身份验证。
`-domain` <*域名*>	指定客户端设备帐户的域。
`-enable`	在指定 View Connection Server 实例中启用 kiosk 模式客户端的身份验证。
`-expirepassword`	指定客户端帐户密码的到期时间与 View Connection Server 组帐户密码到期时间相同。如果没有为该组定义到期时间，则密码不会失效。
`-force`	禁用移除 kiosk 模式客户端帐户时的确认提示。
`-genpassword`	为客户端帐户生成密码。如果您未指定 `-password` 或 `-genpassword`，则会执行此默认行为。
`-getdefaults`	获得添加客户端帐户使用的默认值。
`-group` <*组名*>	指定客户端帐户所加入的默认组的名称。必须按照 Windows 2000 之前版本中组名称的指定方式从 Active Directory 指定组名称。
`-list`	显示 kiosk 模式客户端以及已启用 kiosk 模式客户端身份验证的 View Connection Server 实例的相关信息。
`-noexpirepassword`	指定帐户的密码不会失效。
`-nogroup`	为客户端添加帐户时，指定该客户端的帐户不会被添加到默认组。 为客户端设置默认值时，清除默认组的设置。
`-ou` <*DN*>	指定客户端帐户被添加到的组织单位的可识别名称。 例如：OU=kiosk-ou,DC=myorg,DC=com **注意** 您无法使用 `-setdefaults` 选项更改组织单位的配置。
`-password` "<*密码*>"	为客户端帐户指定显式密码。
`-remove`	移除处于 kiosk 模式的客户端帐户。
`-removeall`	移除所有处于 kiosk 模式的客户端的帐户。
`-requirepassword`	指定处于 kiosk 模式的客户端必须提供密码。View Manager 不接受为新连接生成的密码。
`-s` <*连接服务器*>	指定要启用或禁用 kiosk 模式客户端身份验证的 View Connection Server 实例的 NetBIOS 名称。
`-setdefaults`	设置添加客户端帐户使用的默认值。
`-update`	为 kiosk 模式客户端更新一个帐户。

示例

为客户端的组织单位、密码到期项和组成员设置默认值。

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group
kc-grp
```

获取纯文本格式的当前客户端默认值。

```
vdmadmin -Q -clientauth -getdefaults
```

获取 XML 格式的当前客户端默认值。

```
vdmadmin -Q -clientauth -getdefaults -xml
```

将按其 MAC 地址指定的客户端的帐户添加到 MYORG 域，并将默认设置应用于组 kc-grp。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

将按其 MAC 地址指定的客户端的帐户添加到 MYORG 域，并使用自动生成的密码。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword -ou "OU=kiosk-
ou,DC=myorg,DC=com" -group kc-grp
```

为已命名的客户端添加帐户，并为该客户端指定一个密码。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid Custom-Terminal21 -password "guest" -ou
"OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

更新客户端的帐户，指定一个新密码和描述文本。

```
vdmadmin -Q -clientauth -update -domain MYORG -clientid Custom-Terminal21 -password "Secret1!"-
description "Foyer Entry Workstation"
```

从 MYORG 域中移除根据 MAC 地址指定的 kiosk 模式客户端的帐户。

```
vdmadmin -Q -clientauth -remove -domain MYORG -clientid 00:10:db:ee:54:12
```

在不提示确认移除的情况下直接移除所有客户端的帐户。

```
vdmadmin -Q -clientauth -removeall -force
```

为 View Connection Server 实例 csvr-2 启用客户端身份验证。具有自动生成密码的客户端无需提供密码就可以对自身进行身份验证。

```
vdmadmin -Q -enable -s csvr-2
```

为 View Connection Server 实例 csvr-3 启用客户端身份验证，并要求客户端将其密码指定给 View Client。具有自动生成密码的客户端无法对自身进行身份验证。

```
vdmadmin -Q -enable -s csvr-3 -requirepassword
```

为 View Connection Server 实例 csvr-1 禁用客户端身份验证。

```
vdmadmin -Q -disable -s csvr-1
```

以文本格式显示有关客户端的信息。客户端 cm-00_0c_29_0d_a3_e6 具有自动生成的密码，而且不需要最终用户或应用程序脚本将该密码指定给 View Client。客户端 cm-00_22_19_12_6d_cf 具有显式指定的密码，并需要最终用户提供该密码。View Connection Server 实例 CONSVR2 接受具有自动生成密码的客户端发出的身份验证请求。CONSVR1 不接受来自 kiosk 模式客户端的身份验证请求。

```
C:\ vdmadmin -Q -clientauth -list
Client Authentication User List
===============================
GUID               :94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID           :cm-00_0c_29_0d_a3_e6
```

```
Domain            :myorg.com
Password Generated:true

GUID              :471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID          :cm-00_22_19_12_6d_cf
Domain            :myorg.com
Password Generated:false

Client Authentication Connection Servers
========================================
Common Name                    :CONSVR1
Client Authentication Enabled :false
Password Required              :false

Common Name                    :CONSVR2
Client Authentication Enabled :true
Password Required              :false
```

使用 -R 选项显示桌面的首个用户

您可以使用 vdmadmin 命令和 -R 选项查明受管理桌面的初始分配情况。例如，在丢失 LDAP 数据的情形下，您可能需要此信息，以便重新为用户分配桌面。

语法

vdmadmin -R -i *<网络地址>*

用法说明

您不能使用 -b 选项以特权用户的身份运行此命令。您必须以 **Administrator** 角色登录。

选项

-i 选项指定了桌面的 IP 地址。

示例

显示第一个访问 IP 地址为 10.20.34.120 的计算机的用户。

```
vdmadmin -R -i 10.20.34.120
```

使用 -S 选项移除 View Connection Server 实例条目

您可以使用 vdmadmin 命令和 -S 选项从 View Manager 配置中移除 View Connection Server 实例条目。

语法

vdmadmin -S [-b *<身份验证自变量>*] -r -s *<服务器>*

用法说明

为确保高可用性，您可以利用 View Manager 在 View Connection Server 组中配置一个或多个副本 View Connection Server 实例。如果您禁用组中的一个 View Connection Server 实例，该服务器条目仍会保留在 View Manager 配置中。要永久移除条目，请从服务器中卸载 View 软件并使用 `vdmadmin` 命令从配置中移除该服务器的条目。

如果您想在已移除的系统中重新安装 VMware View，但并不想复制原始组的 View 配置，请在重新安装前重新启动原始组中的所有 View Connection Server 主机。此操作可防止重新安装的 View Connection Server 实例从原始组中接收配置更新。

选项

`-s` 选项指定了要移除的 View Connection Server 实例的 NetBIOS 名称。

示例

移除 View Connection Server 实例 connsvr3 的条目。

```
vdmadmin -S -r -s connsvr3
```

使用 -T 选项设置发布 View Transfer Server 文件包的拆分限制

您可以使用 `vdmadmin` 命令和 `-T` 选项设置发布 View Transfer Server 文件包的拆分限制。如果您使用一个定义了最大缓存目标大小的代理缓存，您可能需要指定拆分限制。

语法

```
vdmadmin -T [-packagelimit <大小>]
```

用法说明

在包含代理缓存的网络中，您可以限制发布的 View Transfer Server 文件包的大小，使其不超过缓存最大目标文件大小，从而提高性能。如果您指定一个拆分限制，View Transfer Server 会将文件包分为不超过此限制的数个部分。

选项

`-packagelimit` 选项指定了拆分限制的字节大小。如果您没有指定此选项，该命令会返回当前的拆分限制。

示例

将拆分限制设置为 10KB。

```
vdmadmin -T -packagelimit 10240
```

显示当前的拆分限制。

```
vdmadmin -T
```

使用 -U 选项显示用户信息

您可以使用 `vdmadmin` 命令和 `-U` 选项显示用户的详细信息。

语法

```
vdmadmin -U [-b <身份验证自变量>] -u <域>\<用户> [-w | -n] [-xml]
```

用法说明

此命令显示从 Active Directory 和 View Manager 中获得的用户的信息。

- Active Directory 中用户帐户的详细信息。
- Active Directory 组的成员身份。
- 桌面授权，包括桌面 ID、显示名称、描述、文件夹，以及桌面是否被禁用。
- ThinApp 分配。
- Administrator 角色，包括用户的管理权限以及他们在哪些文件夹中具有这些权限。

选项

`-u` 选项可指定用户的名称和域。

示例

以 XML 格式（使用 ASCII 字符）显示域 CORP 中用户 Jo 的相关信息。

```
vdmadmin -U -u CORP\Jo -n -xml
```

使用 -V 选项解密本地桌面的虚拟机

VMware View 通过对虚拟机的基础映像进行加密来保护本地桌面的虚拟机。如果无法启动或检入本地桌面，您可以将 `vdmadmin` 命令与 `-V` 选项配合使用对虚拟机进行解密，以便从中恢复数据。

语法

```
vdmadmin -V -rescue [-b <身份验证自变量>] -d <桌面> -u <域>\<用户> -infile <VM 文件路径>
```

用法说明

要解密完整的虚拟机，请从客户端计算机中复制所有的虚拟机文件。作为 `-infile` 选项的自变量，指定 VMware 虚拟机配置文件（VMX 文件）的名称。

要解密虚拟机的某个磁盘，请复制所有与该磁盘相对应的 VMware 虚拟磁盘文件（VMDK 文件）。如果您从链接克隆桌面创建了本地桌面，还必须复制包含基础映像的 VMDK 文件的子文件夹。作为 `-infile` 选项的自变量，为该磁盘指定 VMDK 文件的名称。不要指定与磁盘分区相对应的 VMDK 文件。

`vdmadmin` 命令会将解密的文件写入到一个名为 `rescued` 的子文件夹。

如果正确的身份验证密钥在 View LDAP 配置中不可用，或者所需的虚拟机文件损坏或丢失，则解密操作将会失败。

选项

表 16–15 列出了解密完整的虚拟机或其单个磁盘时必须指定的选项。

表 16–15 解密本地桌面虚拟机的选项

选项	描述
`-d` *<桌面>*	指定桌面池名称。
`-infile` *<VM 文件路径>*	为本地桌面的虚拟机指定 VMX 或 VMDK 文件的路径。
`-u` *<域>\<用户>*	指定本地桌面最终用户的域和名称。

示例

通过指定虚拟机的 VMX 文件来解密整个虚拟机。

```
vdmadmin -V -rescue -d lmdtpool -u MYCORP\jo -infile "J:\Temp\LMDT_Recovery
\CN=lmdtpool,OU=Applications,DC=mycorp,DC=com.vmx"
```

通过指定 VMDK 文件来解密当前版本的虚拟机 `scsi00` 磁盘。

```
vdmadmin -V -rescue -d lmdtpool -u MYCORP\jo -infile "J:\Temp\LMDT_Recovery
\52e52b7c26a2f683-42b945f934e0fbb2-scsi00-000001.vmdk
"
```

使用 -V 选项解锁或锁定虚拟机

您可以使用 `vdmadmin` 命令和 `-V` 选项解锁或锁定数据中心的虚拟机。

语法

```
vdmadmin -V [-b <身份验证自变量>] -e -d <桌面> -m <计算机> [-m <计算机>] ...

vdmadmin -V [-b <身份验证自变量>] -e -vcdn <vCenter DN> -vmpath <详细目录>

vdmadmin -V [-b <身份验证自变量>] -p -d <桌面> -m <计算机> [-m <计算机>] ...

vdmadmin -V [-b <身份验证自变量>] -p -vcdn <vCenter DN> -vmpath <详细目录>
```

用法说明

如果 View 桌面因遇到问题而处于错误状态，您只能使用 `vdmadmin` 命令来解锁或锁定虚拟机。请勿使用此命令管理正常运行的桌面。例如，如果您能使用 View Administrator 回滚本地会话，就不要使用 `vdmadmin` 解锁检出的远程桌面。

如果桌面被锁定且无法回滚，并且 ADAM 中有此桌面的虚拟机条目，请使用 `-d` 和 `-m` 选项为您希望解锁的桌面指定桌面池和虚拟机。您可以使用 `vdmadmin -M` 选项查找分配给用户的虚拟机名称。

如果桌面被锁定，且 ADAM 中没有该桌面的虚拟机条目，请使用 `-vmpath` 和 `-vcdn` 选项指定虚拟机的详细目录和 vCenter Server。您可以使用 vCenter Client 从 `Home/Inventory/VMs and Templates` 中找到桌面或 View Transfer Server 实例的虚拟机详细目录。您可以用 ADAM ADSI Edit 在 `OU=Properties` 标题下找到 vCenter Server 的可识别名称。

选项

表 16-16 显示了解锁或锁定虚拟机时您可以指定的选项。

表 16–16 解锁或锁定虚拟机的选项

选项	描述
`-d` <*桌面*>	指定桌面池。
`-e`	解锁虚拟机。
`-m` <*计算机*>	指定虚拟机名称。
`-p`	锁定虚拟机。
`-vcdn` <*vCenter DN*>	指定 vCenter Server 的可识别名称。
`-vmpath` <*详细目录*>	指定虚拟机的详细目录。

示例

解锁桌面池 dtpool3 中的虚拟机 machine1 和 machine2。

```
vdmadmin -V -e -d dtpool3 -m machine1 -m machine2
```

解锁 vCenter Server 中 View Transfer Server 实例的虚拟机。

```
vdmadmin -V -e -vcdn  "CN=f1060058-
dde2-4940-947b-5d83757b1787,OU=VirtualCenter,OU=Properties,DC=myorg,DC=com" -vmpath "/
DataCenter1/vm/Desktops/LocalMode/LDwin7"
```

锁定桌面池 dtpool3 中的虚拟机 machine3。

```
vdmadmin -V -p -d dtpool3 -m machine3
```

设置 Kiosk 模式的客户端 17

您可以设置从 VMware View 获取桌面访问权限的无人参与运行的客户端。

Kiosk 模式客户端是一个运行 View Client 以连接 View Connection Server 实例并启动远程会话的瘦客户端或锁定 PC。最终用户通常无需登录就可以访问客户端设备，虽然对某些应用程序而言桌面可能需要用户提供身份验证信息。具有代表性的应用程序包括医疗数据条目工作站、航空公司登记站、客户自助服务点和公共访问信息终端。

您应当确保：桌面应用程序可通过身份验证机制保证交易安全、物理网络不会被篡改和偷窃，以及连接到网络的所有设备都是受信任的。

Kiosk 模式的客户端支持远程访问的标准功能，例如将 USB 设备自动重定向到远程会话以及基于位置的打印功能。

View Manager 使用 VMware View 4.5 的灵活身份验证功能对 Kiosk 模式的客户端设备（而非最终用户）进行身份验证。您可以配置 View Connection Server 实例，对以自身 MAC 地址为标识或以字符 "Custom-" 开头的用户名为标识的客户端进行身份验证。如果您将客户端配置为使用自动生成的密码，则无需指定密码即可以在设备上运行 View Client。如果您配置显式密码，则必须将该密码指定给 View Client。由于您通常要从脚本运行 View Client，而密码在脚本中清晰可见，因此您应该设法防止未得到授权的用户读取该脚本。

只有您用来对 Kiosk 模式客户端进行身份验证的 View Connection Server 实例才能接受以字符 "cm-" 开头并后接 MAC 地址（或以字符 "Custom-" 开头）的帐户发出的连接。VMware View 4.5 中的 View Client 不允许手动输入采用这两种格式的用户名。

最好的办法是使用专用的 View Connection Server 实例处理 Kiosk 模式的客户端，并在 Active Directory 中为这些客户端的帐户创建专用的组织单位和组。这样不仅能防止这些系统遭受意外入侵，还会使客户端的配置和管理变得更加容易。

配置 Kiosk 模式的客户端

要配置 Active Directory 和 View Manager 来支持 Kiosk 模式的客户端，您必须按顺序执行若干任务。

前提条件

确认您有执行配置任务所需的特权。

- **Active Directory 中的 Domain Admins** 或 **Account Operators** 凭据，以对域中的用户和组帐户进行更改。
- **Administrators**、**Inventory Administrators** 或等效角色，以使用 View Administrator 将用户或组授权给桌面。
- **Administrators** 或等效角色，以运行 `vdmadmin` 命令。

步骤

1 为 Kiosk 模式客户端准备 Active Directory 和 View Manager 第 294 页，

   您必须配置 Active Directory 来接受您所创建的用来对客户端设备进行身份验证的帐户。无论何时创建组，都必须将该组授权给客户端访问的桌面池。您还可以准备客户端使用的桌面池。

2 为 Kiosk 模式客户端设置默认值第 295 页，

   您可以使用 vdmadmin 命令在 Active Directory 中为 Kiosk 模式客户端的组织单位、密码到期项和组成员设置默认值。

3 显示客户端设备的 MAC 地址第 296 页，

   如果您想为客户端创建基于其 MAC 地址的帐户，可以使用 View Client 找出该客户端设备的 MAC 地址。

4 为 Kiosk 模式客户端添加帐户第 296 页，

   您可以使用 vdmadmin 命令将客户端的帐户添加到 View Connection Server 组的配置中。添加的客户端可在启用了客户端身份验证的 View Connection Server 实例中使用。您还可以更新客户端的配置，或者从系统中移除其帐户。

5 启用 Kiosk 模式客户端的身份验证第 297 页，

   您可以使用 vdmadmin 命令对尝试通过 View Connection Server 实例连接桌面的客户端进行身份验证。

6 验证 Kiosk 模式客户端的配置第 298 页，

   您可以使用 vdmadmin 命令显示 Kiosk 模式客户端以及为对这些客户端进行身份验证而配置的 View Connection Server 实例的信息。

7 从 Kiosk 模式客户端连接到桌面第 299 页，

   您可以从命令行运行 View Client 或使用脚本将客户端连接到远程会话。

为 Kiosk 模式客户端准备 Active Directory 和 View Manager

您必须配置 Active Directory 来接受您所创建的用来对客户端设备进行身份验证的帐户。无论何时创建组，都必须将该组授权给客户端访问的桌面池。您还可以准备客户端使用的桌面池。

作为最佳实践，请创建一个单独的组织单位和组，尽可能减少管理 Kiosk 模式客户端的工作。您可以为不属于任何组的客户端添加单独的帐户，但如果您配置大量客户端，就会带来大量的管理开销。

步骤

1 在 Active Directory 中，创建一个单独的组织单位和组以供 Kiosk 模式客户端使用。

   您必须为该组指定一个 Windows 2000 版本之前的名称。您需要使用此名称在 vdmadmin 命令中标识该组。

2 为客户虚拟机创建映像或模板。

   您可以将 vCenter Server 管理的虚拟机用作自动池的模板、链接克隆池的父虚拟机或者手动池的桌面源。您还可以在客户虚拟机上安装和配置应用程序。

3 配置客户虚拟机，以便当客户端在无人参与状态下运行时不被锁定。

   View 禁止为以 Kiosk 模式连接的客户端显示登录前的消息。如果需要一个能够解锁屏幕和显示消息的事件，可以在客户虚拟机上配置一个合适的应用程序。

4 在 View Administrator 中，创建客户端将使用的桌面池并将组授权给该池。

   例如，您可以选择创建一个最能满足客户端应用程序要求的浮动分配链接克隆桌面池。您还可将一个或多个 ThinApp 应用程序关联到桌面池。

   重要事项 不要将客户端或组授权给多个桌面池。这会使 View Manager 从已授权客户端的池随机分配桌面，并生成一个警告事件。

5 如果您想为客户端启用基于位置的打印功能，可以配置 Active Directory 组策略设置 [AutoConnect Location-based Printing for VMware View（为 VMware View 自动连接基于位置的打印）]，该设置位于 Microsoft 组策略对象编辑器 **[Computer Configuration（计算机配置）]** 下的 **[Software Settings（软件设置）]** 文件夹中。

6 配置优化和保护客户端的 View 桌面所需的其他策略。

   例如，您可能希望覆盖在启动或插入本地 USB 设备时将其连接到桌面这一策略。默认情况下，适用于 Windows 的 View Client 会对 Kiosk 模式客户端启用这些策略。

示例 17–1 为 Kiosk 模式客户端准备 Active Directory

公司内网中包含域 MYORG，且它的组织单位具有可区分的名称 OU=myorg-ou,DC=myorg,DC=com。在 Active Directory 中，您需要创建拥有可区分名称 OU=kiosk-ou,DC=myorg,DC=com 的组织单位 kiosk-ou 以及组 kc-grp，以供 Kiosk 模式客户端使用。

下一步

为客户端设置默认值。

为 Kiosk 模式客户端设置默认值

您可以使用 vdmadmin 命令在 Active Directory 中为 Kiosk 模式客户端的组织单位、密码到期项和组成员设置默认值。

您必须在客户端用来连接其桌面的 View Connection Server 实例所在组中的一个 View Connection Server 实例上运行 vdmadmin 命令。

当您为密码到期项和 Active Directory 组成员关系配置默认值时，这些设置会由组中所有的 View Connection Server 实例共享。

步骤

◆ 为客户端设置默认值。

```
vdmadmin -Q -clientauth -setdefaults [-b <身份验证自变量>] [-ou <DN>] [ -expirepassword |
-noexpirepassword ] [-group <组名> | -nogroup]
```

选项	描述
-expirepassword	指定客户端帐户密码的到期时间与 View Connection Server 组的到期时间相同。如果没有为该组定义到期时间，则密码不会失效。
-group <*组名*>	指定客户端帐户所加入的默认组的名称。组名必须指定为 Windows 2000 之前版本的 Active Directory 组名。
-noexpirepassword	将客户端帐户的密码指定为从不过期。
-nogroup	清除默认组的设置。
-ou <*DN*>	指定客户端帐户所加入的默认组织单位的可区分名称。 例如：OU=kiosk-ou,DC=myorg,DC=com **注意** 您无法使用该命令更改组织单位的配置。

该命令可更新 View Connection Server 组中客户端的默认值。

示例 17–2 为 Kiosk 模式客户端设置默认值

为客户端的组织单位、密码到期项和组成员设置默认值。

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group
kc-grp
```

下一步

找出使用自身 MAC 地址进行身份验证的客户端设备的 MAC 地址。

显示客户端设备的 MAC 地址

如果您想为客户端创建基于其 MAC 地址的帐户，可以使用 View Client 找出该客户端设备的 MAC 地址。

前提条件

登录客户端控制台。

步骤

◆ 要显示 MAC 地址，请根据您所用的平台键入相应的命令。

选项	操作
Windows	输入 **`C:\Program Files\VMware\VMware View\Client\bin\wswc -printEnvironmentInfo`** View Client 使用您为其配置的默认 View Connection Server 实例。如果您尚未配置默认值，View Client 会提示您配置该值。 该命令可显示客户端设备的 IP 地址、MAC 地址和计算机名称。
Linux	输入 **`vmware-view --printEnvironmentInfo -s`** ***<连接服务器>*** 您必须指定 View Client 连接桌面时使用的 View Connection Server 实例的 IP 地址或 FQDN。 该命令可显示 IP 地址、MAC 地址、计算机名称、域、任何登录用户的名称和域，以及客户端设备的时区。

下一步

为客户端添加帐户。

为 Kiosk 模式客户端添加帐户

您可以使用 `vdmadmin` 命令将客户端的帐户添加到 View Connection Server 组的配置中。添加的客户端可在启用了客户端身份验证的 View Connection Server 实例中使用。您还可以更新客户端的配置，或者从系统中移除其帐户。

您必须在客户端用来连接其桌面的 View Connection Server 实例所在组中的一个 View Connection Server 实例上运行 `vdmadmin` 命令。

添加 Kiosk 模式客户端时，View Manager 会在 Active Directory 中为该客户端创建一个用户帐户。如果为客户端指定名称，则该名称必须以字符 "Custom-" 开头，而且名称长度不得超过 20 个字符。如果您没有为客户端指定名称，View Manager 将通过您为客户端设备指定的 MAC 地址生成一个名称。例如，如果 MAC 地址是 00:10:db:ee:76:80，则相应的帐户名是 cm-00_10_db_ee_76_80。您只能在用来对客户端进行身份验证的 View Connection Server 实例中使用这些帐户。

重要事项 不要将一个指定的名称用于多个客户端设备。今后的版本可能不支持该配置。

步骤

◆ 使用 `-domain` 和 `-clientid` 选项运行 `vdmadmin` 命令，指定客户端所在的域及其名称或 MAC 地址。

```
vdmadmin -Q -clientauth -add [-b <身份验证自变量>] -domain <域名> -clientid <客户端 ID>
[-password "<密码>" | -genpassword] [-ou <DN>] [-expirepassword | -noexpirepassword] [-group <
组名> | -nogroup] [-description "描述文本"]
```

选项	描述
`-clientid` ***<客户端 ID>***	指定客户端的名称或 MAC 地址。
`-description` **"*描述文本*"**	在 Active Directory 中为客户端设备创建帐户描述。

选项	描述
-domain <*域名*>	指定客户端的域。
-expirepassword	指定客户端帐户密码的到期时间与 View Connection Server 组的到期时间相同。如果没有为该组定义到期时间，则密码永远不会到期。
-genpassword	为客户端帐户生成密码。如果您未指定 `-password` 或 `-genpassword`，则会执行此默认行为。 生成的密码长度是 16 位，至少包含一个大写字母、一个小写字母、一个符号和一个数字，可以包含重复字符。如果您需要一个更强的密码，请使用 `-password` 选项指定密码。
-group <*组名*>	指定要添加客户端帐户的组的名称。组名必须指定为 Windows 2000 之前版本的 Active Directory 组名。 如果您之前设置了默认组，则客户端帐户会被添加到该组。
-noexpirepassword	将客户端帐户的密码指定为永不过期。
-nogroup	指定不将客户端帐户添加到默认组。
-ou <*DN*>	指定要添加客户端帐户的组织单位的可区分名称。 例如：OU=kiosk-ou,DC=myorg,DC=com
-password "<*密码*>"	为客户端帐户指定显式密码。

该命令会在 Active Directory 中为指定的域和组（如果存在）中的客户端创建一个用户帐户。

示例 17–3 为客户端添加帐户

使用组 kc-grp 的默认设置，将由 MAC 地址指定的客户端帐户添加到 MYORG 域。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

使用自动生成的密码，将由 MAC 地址指定的客户端帐户添加到 MYORG 域。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

为已命名的客户端添加帐户，并为该客户端指定一个密码。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid Custom-Terminal21 -password "guest" -ou
"OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

使用自动生成的密码为命名的客户端添加帐户。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid Custom-Kiosk11 -ou "OU=kiosk-
ou,DC=myorg,DC=com" -description "Kiosk 11"
```


下一步

启用客户端身份验证。

启用 Kiosk 模式客户端的身份验证

您可以使用 `vdmadmin` 命令对尝试通过 View Connection Server 实例连接桌面的客户端进行身份验证。

您必须在客户端用来连接其桌面的 View Connection Server 实例所在组中的一个 View Connection Server 实例上运行 `vdmadmin` 命令。

虽然您是为单个 View Connection Server 实例启用身份验证，但是组中的所有 View Connection Server 实例都会共享客户端身份验证的所有其他设置。您仅需为每个客户端添加一个帐户。在 View Connection Server 组中，任何启用的 View Connection Server 实例都可对该客户端进行身份验证。

步骤

◆ 在 View Connection Server 实例上启用客户端身份验证。

```
vdmadmin -Q -enable [-b <身份验证自变量>] -s <连接服务器> [-requirepassword]
```

选项	描述
`-requirepassword`	指定该选项即表示您需要客户端提供密码。 **重要事项** 如果您指定该选项，View Connection Server 实例将无法对具有自动生成密码的客户端进行身份验证。如果您更改 View Connection Server 实例的配置来指定该选项，此类客户端将无法对自身进行身份验证，而且会返回错误消息 `Unknown username or bad password`（未知用户名或无效密码）。
-s *<连接服务器>*	指定要启用客户端身份验证的 View Connection Server 实例的 NetBIOS 名称。

该命令可使指定的 View Connection Server 实例对客户端进行身份验证。

示例 17–4 启用 Kiosk 模式客户端的身份验证

为 View Connection Server 实例 csvr-2 启用客户端身份验证。具有自动生成密码的客户端无需提供密码就可以对自身进行身份验证。

```
vdmadmin -Q -enable -s csvr-2
```

为 View Connection Server 实例 csvr-3 启用客户端身份验证，并要求客户端将其密码指定给 View Client。具有自动生成密码的客户端无法对自身进行身份验证。

```
vdmadmin -Q -enable -s csvr-3 -requirepassword
```

下一步

确认 View Connection Server 实例和客户端的配置。

验证 Kiosk 模式客户端的配置

您可以使用 `vdmadmin` 命令显示 Kiosk 模式客户端以及为对这些客户端进行身份验证而配置的 View Connection Server 实例的信息。

您必须在客户端用来连接其桌面的 View Connection Server 实例所在组中的一个 View Connection Server 实例上运行 `vdmadmin` 命令。

步骤

◆ 显示有关 Kiosk 模式客户端和客户端身份验证的信息。

```
vdmadmin -Q -clientauth -list [-b <身份验证自变量>] [-xml]
```

该命令可显示有关 Kiosk 模式客户端以及启用了客户端身份验证的 View Connection Server 实例的信息。

示例 17–5 显示 Kiosk 模式客户端的信息

以文本格式显示有关客户端的信息。客户端 cm-00_0c_29_0d_a3_e6 具有自动生成的密码，而且不需要最终用户或应用程序脚本将该密码指定给 View Client。客户端 cm-00_22_19_12_6d_cf 具有显式指定的密码并需要最终用户提供该密码。View Connection Server 实例 CONSVR2 接受具有自动生成密码的客户端发出的身份验证请求。CONSVR1 不接受来自 Kiosk 模式客户端的身份验证请求。

```
C:\ vdmadmin -Q -clientauth -list
Client Authentication User List
===============================
GUID              :94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID          :cm-00_0c_29_0d_a3_e6
Domain            :myorg.com
Password Generated:true

GUID              :471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID          :cm-00_22_19_12_6d_cf
Domain            :myorg.com
Password Generated:false

Client Authentication Connection Servers
========================================
Common Name                  :CONSVR1
Client Authentication Enabled :false
Password Required            :false

Common Name                  :CONSVR2
Client Authentication Enabled :true
Password Required            :false
```

下一步

确认客户端可以连接到其桌面。

从 Kiosk 模式客户端连接到桌面

您可以从命令行运行 View Client 或使用脚本将客户端连接到远程会话。

您通常会在部署的客户端设备上使用命令脚本来运行 View Client。

有关在 Windows 系统上运行 View Client 的脚本示例，请查看文件 `C:\Program Files\VMware\VMware View \Client\bin\kiosk_mode.cmd`。

注意 在 Windows 客户端上，如果在桌面会话启动时客户端上的 USB 设备正被另一个应用程序或服务使用，则这些 USB 设备无法被自动转发。您必须确保在客户端上为希望转发的所有设备安装驱动程序。在 Windows 和 Linux 客户端上，默认情况下不转发人机界面设备 (HID) 和智能卡读卡器。

步骤

◆ 要连接到远程会话，请在您的平台上键入相应的命令。

选项	描述	
Windows	输入 **C:\Program Files\VMware\VMware View\Client\bin\wswc -unattended [-serverURL *<连接服务器>*] [-userName *<用户名>*] [-password *<密码>*]**	
	-password <*密码*>	为客户端帐户指定密码。如果您为该帐户定义了密码，则必须指定该密码。
	-serverURL <*连接服务器*>	指定 View Client 在连接桌面时所用的 View Connection Server 实例的 IP 地址或 FQDN。如果您未指定 View Client 在连接桌面时所用的 View Connection Server 实例的 IP 地址或 FQDN，View Client 将使用您为它配置的默认 View Connection Server 实例。
	-userName <*用户名*>	指定客户端帐户名称。如果您想让客户端使用一个以字符 "Custom-" 开头的帐户名（而非其 MAC 地址）对自身进行身份验证，则必须指定该名称。
Linux	输入 **vmware-view --unattended -s *<连接服务器>* [--once] [-u *<用户名>*] [-p *<密码>*]**	
	--once	指定此选项，可以在发生错误时避免 View Client 重新尝试连接。 **重要事项** 通常情况下，您应该指定该选项，并利用退出代码来处理错误。否则，您将在远程终止 vmware-view 进程时遇到困难。
	-p <*密码*>	为客户端帐户指定密码。如果您为该帐户定义了密码，则必须指定该密码。
	-s <*连接服务器*>	指定 View Client 在连接桌面时所用的 View Connection Server 实例的 IP 地址或 FQDN。
	-u <*用户名*>	指定客户端帐户名称。如果您想让客户端使用一个以字符 "Custom-" 开头的帐户名（而非其 MAC 地址）对自身进行身份验证，则必须指定该名称。

如果 View Manager 对 Kiosk 客户端进行了身份验证并且有 View 桌面可用，该命令会启动远程会话。

示例 17–6 在 Kiosk 模式客户端上运行 View Client

在帐户名基于自身 MAC 地址、且具有自动生成密码的 Windows 客户端上运行 View Client。

```
C:\Program Files\VMware\VMware View\Client\bin\wswc -unattended -serverURL consvr2.myorg.com
```

使用分配的名称和密码在 Linux 客户端上运行 View Client。

```
vmware-view -unattended -s 145.124.24.100 --once -u Custom-Terminal21 -p "Secret1!"
```

通过命令行运行 View Client 18

您可以通过命令行或脚本运行 Windows View Client。如果您正运行一个基于 Kiosk 的应用程序， 而此应用程序为最终用户授予桌面应用程序的访问权限，可能会希望执行此操作。

您可以在命令行执行 wswc 命令运行 Windows View Client。该命令包括一些选项，您可以指定这些选项来改变 View Client 的行为。

本章讨论了以下主题：

View Client 命令用法

wswc 命令语法可控制 View Client 的运行。

在 Windows 命令提示符下，使用以下 wswc 命令格式。

```
wswc [<命令行选项> [<自变量>]] ...
```

您指定的命令行选项可以改变 View Client 的行为。

默认情况下，wswc 命令可执行文件位于 `C:\Program Files\VMware\VMware View\Client\bin\wswc.exe`。为方便起见，请将该路径添加到 *PATH* 环境变量中。

表 18–1 显示了可与 wswc 命令一起使用的命令行选项。

表 18–1 View Client 命令行选项

选项	描述
/?	显示命令选项列表。
-checkin	（仅适用于本地桌面）检入指定的桌面并解锁相应的联机桌面。 该选项需要您同时指定 -desktopName 选项。
-checkout	（仅适用于本地桌面）检出指定的桌面并锁定相应的联机桌面。
-confirmRollback	（仅适用于本地桌面）禁止在使用 -rollback 选项时出现确认对话框。要以非交互模式执行回滚，还需要指定 -nonInteractive 选项。
-connectUSBOnStartup	将所有 USB 设备重定向到当前连接至主机的桌面。如果您指定了 -unattended 选项，则会隐式设置该选项。
-connectUSBOnInsert	插入 USB 设备时，将其连接到前台桌面。如果您指定了 -unattended 选项，则会隐式设置该选项。

表 18–1 View Client 命令行选项 （续）

选项	描述
`-desktopLayout` *窗口大小*	指定如何显示桌面窗口： **`fullscreen`** 全屏显示 **`multimonitor`** 多显示器显示 **`windowLarge`** 大窗口 **`windowSmall`** 小窗口
`-desktopName` *<桌面名>*	指定桌面在 [Select Desktop（选择桌面）] 对话框中的显示名称。这将是您在选择桌面对话框中看到的桌面名称。
`-desktopProtocol` *<协议>*	指定 [Select Desktop（选择桌面）] 对话框中显示的可用桌面协议。可以是 PCOIP、RDP 或 RGS 协议。
`-domainName` *<域名>*	指定最终用户用来登录到 View Client 的域。
`-file` *<文件路径>*	指定包含其他命令选项和自变量的配置文件的路径。请参阅 第 303 页，“View Client 配置文件”。
`-languageId` *<区域 ID>*	在 View Client 中提供对不同语言的本地化支持。如果资源库可用，指定要使用的 Locale ID (LCID)。对于美国英语，输入的值为 0x409。
`-localDirectory` *目录路径*	（仅适用于本地桌面）指定使用本地系统上的哪个目录来下载本地桌面。 该选项需要您同时指定 `-desktopName` 选项。
`-logInAsCurrentUser`	使用最终用户在登录客户端系统时提供的凭据信息登录 View Connection Server 实例，并最终登录到 View 桌面。
`-nonInteractive`	通过脚本启动 View Client 时禁止显示错误消息框。如果您指定了 `-unattended` 选项，则会隐式设置该选项。
`-password` *<密码>*	指定最终用户登录 View Client 时使用的密码。如果您自动生成密码，则无需为 Kiosk 模式客户端指定该选项。
`-printEnvironmentInfo`	显示客户端设备的 IP 地址、MAC 地址和计算机名称。
`-repairLocalDesktops`	（仅适用于本地桌面）尝试修复本地桌面的虚拟磁盘。如果在磁盘映像正在更新时断开连接或者关闭客户端计算机，可能需要修复虚拟磁盘。执行修复过程可能需要几分钟时间。
`-rollback`	（仅适用于本地桌面）解锁已检出桌面的联机版本并放弃本地会话。 该选项需要您同时指定 `-desktopName` 选项。 要以非交互模式执行回滚，还需要指定 `-nonInteractive` 选项和 `-confirmRollback` 选项。
`-serverURL` *<连接服务器>*	指定 View Connection Server 实例的 URL、IP 地址或 FQDN。
`-smartCardPIN` *<PIN>*	指定最终用户插入智能卡进行登录时所用的 PIN。
`-unattended`	以适用于 Kiosk 模式客户端的非交互模式运行 View Client。您还必须指定： ■ 客户端的帐户名（如果您未根据客户端设备的 MAC 地址生成帐户名）。该名称必须以字符串 "Custom-" 开头。 ■ 客户端的密码（如果您在设置客户端帐户时未自动生成密码）。 `-unattended` 选项可隐式设置 `-nonInteractive`、`-connectUSBOnStartup` 和 `-connectUSBOnInsert` 选项。
`-userName` *<用户名>*	指定最终用户登录 View Client 时使用的帐户名。如果您从客户端设备的 MAC 地址生成帐户名，则无需为 Kiosk 模式客户端指定该选项。

您通过命令行或配置文件指定的选项优先于已定义的任何全局系统策略，进而会覆盖用户策略。

您可以通过 Active Directory 组策略指定所有选项，但 `-checkin`、`-checkout`、`-file`、`-languageId`、`-localDirectory`、`-printEnvironmentInfo`、`-rollback`、`-smartCardPIN` 和 `-unattended` 除外。

View Client 配置文件

您可以从配置文件读取 View Client 的命令行选项。

您可以作为 `wswc` 命令 `-f` 选项的一个自变量来指定配置文件的路径。该文件必须是 Unicode (UTF-16) 或 ASCII 文本文件。

示例 18‑1 非交互式应用程序的配置文件示例

以下示例显示了非交互式应用程序的配置文件内容。

```
-serverURL https://view.yourcompany.com
-userName autouser
-password auto123
-domainName companydomain
-desktopName autodesktop
-nonInteractive
```

示例 18‑2 Kiosk 模式客户端的配置文件示例

以下为 Kiosk 模式客户端示例，示例中的客户端帐户名基于客户端 MAC 地址，且客户端具有一个自动生成的密码。

```
-serverURL 145.124.24.100
-unattended
```

View Client 注册表设置

您可以在 Windows 注册表中定义 View Client 的默认设置，而不必在命令行指定这些设置。

表 18‑2 显示了 View Client 的注册表设置。所有设置都位于注册表的 `HKLM\Software\VMware, Inc.\VMware VDM\Client\` 下。

策略条目优先于注册表设置，命令行设置优先于策略条目。

表 18‑2 View Client 注册表设置

注册表设置	描述
`DomainName`	指定默认域名。
`EnableShade`	指定是否启用 View Client 窗口顶部的菜单栏（幕帘）。默认情况下，该菜单栏已启用，但 Kiosk 模式客户端除外。将值设为 false 可禁用该菜单栏。
`Password`	指定默认密码。
`ServerURL`	通过 URL、IP 地址或 FQDN 指定默认的 View Connection Server 实例。
`UserName`	指定默认用户名。

View Client 退出代码

`wswc` 命令可以返回退出代码来表明 View Client 所遇错误的性质。

表 18‑3 显示了 `wswc` 命令可以返回的退出代码。

表 18‑3 View Client 退出代码

退出代码	描述
-1	Kiosk 模式出现致命错误。
0	成功。
1	连接失败。

表 18–3 View Client 退出代码 （续）

退出代码	描述
2	登录失败。
3	桌面无法启动。
4	RDP 无法启动。
5	RDP 操作失败。
6	安全加密链路连接丢失。
7	本地桌面传输失败。
8	本地桌面检入失败。
9	本地桌面检出失败。
10	本地桌面回滚失败。
11	进行身份验证时接收到未知结果。
12	身份验证错误。
13	接收到使用未知身份验证方法的请求。
14	无效的服务器响应。
15	桌面已断开连接。
16	安全加密链路已断开连接。
17	保留用于今后开发。
18	保留用于今后开发。
19	不支持的 Kiosk 操作。
20	远程鼠标、键盘或屏幕 (RMKS) 连接错误。
21	PIN 错误。
22	PIN 不匹配。
23	密码不匹配。
24	View Connection Server 错误。
25	桌面不可用。

索引